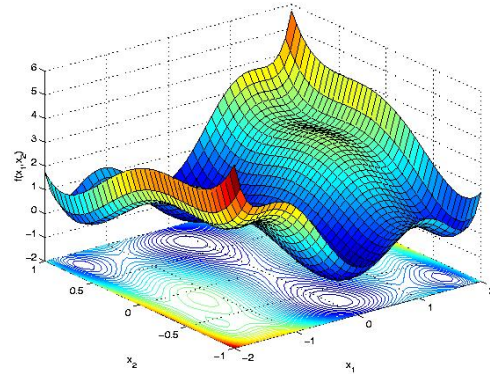
Un voyage avec les polynômes, entre algèbre et optimisation

Journée sur l'Enseignements des maths et de l'info à la FST

Simone Naldi

XLIM – Université de Limoges

14 juin 2022



Deux mathématiciens

H. Minkowski (1864-1909)

D. Hilbert (1862-1943)

Un peu d'histoire

1881 : l'*Académie des Sciences* pose le problème de detérminer le nombre de représentations d'un entier positif comme somme de cinq carrés

1883 : Minkowski (à 18 ans) reçoit le prix de l'Académie ex-æquo[1]

1885 : Minkowski défend sa thèse intitulée

"Untersuchungen über quadratische Formen Bestimmung der Anzahl verschiedener Formen, welche ein gegebenes Genus enthält"

à la fin de sa soutenance, Minkowski affirme[2] que

≪ *Il n'est pas vraisemblable que chaque forme positive soit représentable par une somme de carrés de formes* ≫

1887 : *privatdozent* à Bonn, thèse d'habilitation

Ensuite professeur à Bonn, Königsberg, Zürich, Göttingen.

[1] Conférence "Un texte, un mathématicien" du par Eva Bayer-Fluckiger (lien)

[2] D. Hilbert. *Hermann Minkowski*, Math. Ann. 68:445–471 (1910)

Conjecture de Minkowski $\rightarrow$ Théorème de Hilbert

$\mathbb{R}[x_1, \ldots, x_n]$ anneau des polynômes[3] réels en plusieurs variables $x_1, \ldots, x_n$

$\mathcal{P}_{n,2d} \subset \mathbb{R}[x_1, \ldots, x_n]$ l'ensemble (cône) des polynômes globalement positifs de degré $2d$

$\Sigma_{n,2d} \subset \mathbb{R}[x_1, \ldots, x_n]$ l'ensemble (cône) des sommes de carrées de degré $2d$ $\quad (\Sigma_{n,2d} \subset \mathcal{P}_{n,2d})$

Théorème (Hilbert, 1888) Tous polynômes positifs sont sommes de carrés ($\Sigma_{n,2d} = \mathcal{P}_{n,2d}$) exactement dans les trois cas suivants:

- $n = 1$ (une seule variable) — TFA + $\mathbb{R}$
- $d = 1$ (formes quadratiques) — diagonalisation
- $n = 2$ et $d = 2$ (quartiques planaires) — preuve de Hilbert (non-constructive)

Les premiers contrexemples apparurent dans les années 1960.

[3] Un polynôme réel est un élément de la forme $f = \sum c_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, par exemple $f = 2xy^2z + 1 - 5x^7$

Preuve dans les cas simples (niveau L2/L3)

Polynômes univariés $(n = 1)$.
Si $f \in \mathcal{P}_{1,2d}$, et $\alpha_i \in \mathbb{R}$ et $\beta_j \in \mathbb{C} \setminus \mathbb{R}$ sont les racines de f, alors :

$$f = \prod_{i=1}^{r}(x - \alpha_i)^2 \cdot \prod_{j=1}^{c}(x - \beta_j)(x - \overline{\beta_j}) = g^2 \cdot h\overline{h} = g^2(\mathsf{Re}(h)^2 + \mathsf{Im}(h)^2) \quad \in \Sigma_{1,2d}$$

Formes quadratiques $(d = 1)$.
Si $f = x^T M x$, où $x = (x_1, \ldots, x_n)$, alors les valeurs propres λ_i de $M = M^T$ sont ≥ 0 et

$$f = x^T M x = x^T (P^T D P) x = \sum_{i=1}^{n} \lambda_i (Px)_i^2 \quad \in \Sigma_{n,2}$$

Quartiques planaires $(n = 2, d = 2)$.
Cas non-triviale.

Exemples dans $\mathcal{P}_{n,2d} \setminus \Sigma_{n,2d}$

Motzkin (Ineq., 1967) $n = 2, d = 3$

$$M = 1 + x^4y^2 + x^2y^4 - 3x^2y^2 \quad \in \mathcal{P}_{2,6} \setminus \Sigma_{2,6}$$

Robinson (Math. Soc. 1969) $n = 3, d = 2$

$$R = 1 + x^2y^2 + y^2z^2 + z^2x^2 - 4xyz \quad \in \mathcal{P}_{3,4} \setminus \Sigma_{3,4}$$

Choi et Lam (J. Algebra, 1980) $n = 2, d = 3$

$$CL = x^4y^2 + y^4 + x^2 - 3x^2y^2 \quad \in \mathcal{P}_{2,6} \setminus \Sigma_{2,6}$$

Dixseptième problème de Hilbert

Dans la liste des 23 problèmes, le $17^{ème}$ pose la question d'exprimer

≪ *... une fonction (rationnelle) non-négative comme quotient de sommes de carrées.* ≫

Théorème (Artin, 1927[4]) Tout polynôme positif $f \in \mathcal{P}_{n,2d}$ est somme de carrés de fonctions rationnelles:

$$f = \frac{g_1^2}{h_1^2} + \frac{g_2^2}{h_2^2} + \cdots + \frac{g_r^2}{h_r^2}$$

Autrement dit, on peut toujours "certifier" la positivité de $f \in \mathbb{R}[x_1, \ldots, x_n]$, en calculant une telle représentation dans le corps des fractions $\mathbb{R}(x_1, \ldots, x_n)$.

[4] *Über die Zerlegung definiter Funktionen in Quadrate.* Hamb. Abh. 5:100–115 (1927)

Rationalité

Hilbert précise[5] que en général

≪ *... il est souhaitable, pour certaines questions comme la possibilité de certaines constructions géométriques, de savoir si les coefficients des formes utilisées dans l'expression peuvent toujours être pris dans le domaine de rationalité engendré par les coefficients de la forme représentée.* ≫

Théorème (Scheiderer, 2016[6]) Il existe des polynômes $f \in \mathbb{Q}[x_1, \ldots, x_n] \cap \Sigma_{n,2d}$, qui ne sont pas somme de carrés de polynômes dans $\mathbb{Q}[x_1, \ldots, x_n]$.

Exemple. $x^4 + xy^3 + y^4 - 3x^2yz - 4xy^2z + 2x^2z^2 + xz^3 + yz^3 + z^4 =$

$$\tfrac{1}{4}(2x^2 - \beta y^2 + yz + (2 - \beta^{-1})z^2)^2 + \tfrac{\beta}{4}(2xy + \beta^{-1}y^2 - 2\beta^{-1}xz - \beta yz - z^2)^2$$

où $\beta^3 - 4\beta + 1 = 0, \beta \geq 0.$

[5] [Bochnak, Coste, Roy] *Géométrie algébrique réelle.* Springer-Verlag Ed.1 (1987)

[6] *Sums of squares of polynomials with rational coefficients.* J. European Math. Soc. 18, 1495-1513 (2016)

Le calcul d'un certificat ...

Exemple. Soit $f = x^4 + x^2y^2 + y^4 \in \Sigma_{2,4}$. Il est déjà sous forme "somme de carrés", mais ... il existe une *infinité* de telles représentations:

$$f = v^T A v = \underbrace{\begin{bmatrix} x^2 & xy & y^2 \end{bmatrix}}_{v^T} \underbrace{\begin{bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \lambda_{12} & \lambda_{22} & \lambda_{23} \\ \lambda_{13} & \lambda_{23} & \lambda_{33} \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x^2 \\ xy \\ y^2 \end{bmatrix}}_{v} \quad \Rightarrow \quad A = \begin{bmatrix} 1 & 0 & \lambda \\ 0 & 1-2\lambda & 0 \\ \lambda & 0 & 1 \end{bmatrix}$$

Si λ est tel que $A \succeq 0$ (semi-définie positive = valeurs propres non-négatives) alors une factorisation de $A = U^T U$ nous donne une décomposition en sommes de carrés:

$$f = v^T A v = v^T U^T U v = \|Uv\|^2$$

Pour cet exemple l'ensemble des certicats est l'intervalle $[-1, \frac{1}{2}]$.

Pour $\lambda = 0$ on retrouve le certificat $f = (x^2)^2 + (xy)^2 + (y^2)^2$.

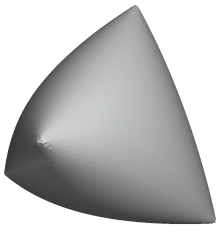
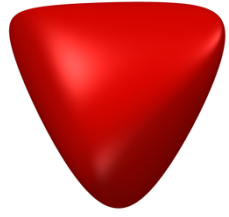
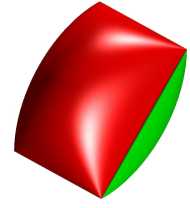
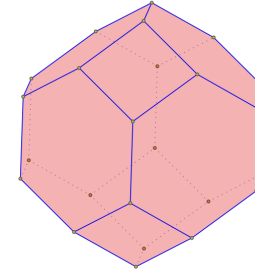
Pour $\lambda = -1$ et $\lambda = 1/2$, on retrouve une somme de *deux* carrés

... c'est un problème d'optimisation !

Le calcul d'un cértificat somme de carrés est un problème appélé **optimisation semi-définie** :

$$\begin{array}{rll} p^* = & \inf & \mathsf{Trace}(CX) \\ & t.q. & \mathsf{Trace}(A_i X) = b_i \\ & & X \succeq 0 \end{array}$$

L'ensemble admissible est *convexe* et est appélé **spectraèdre** (= polyèdre dans le spectre):

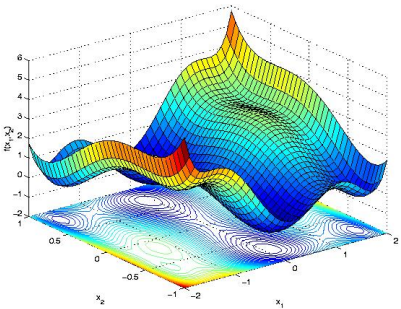





Optimisation avec les polynômes

Soient $g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_n]$. On appelle *ensemble semi-algébrique* :

$$K = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

- Calculer le minimum d'un polynôme sur K (*optimisation polynomiale*)
- Certifier qu'un polynôme est positif sur K



$$\begin{array}{llcll} \inf & f(x) & = & \sup & \lambda \\ t.q. & x \in K & & t.q. & f(x) - \lambda \text{ est positif sur } K \end{array}$$

≪ L'infimum d'une fonction n'est rien d'autre que la plus grande borne inférieure ≫

Théorème de positivité locale (Positivstellensätze)

Quelle est la forme d'un polynôme qui est positifs sur un ensemble semi-algébrique ?

Théorème (Putinar, 1993[7]) Soit $K = \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$ un ensemble semi-algébrique compacte[8]. Alors $f > 0$ sur K si et seulement si

$$f = \sigma_0 + \sigma_1 g_1 + \sigma_2 g_2 + \cdots + \sigma_m g_m, \quad \exists\, \sigma_i \in \Sigma_{n,2d}$$

Il existe une dizaine de théorèmes de positivité pour des ensembles K spécifiques

- intervalles
- orthant positif, polyèdres ...
- sphères, hypercubes, ...

[7] *Positive polynomials on compact semialgebraic sets.* Indiana Univ. Math. 42:969–984 (1993)

[8] Plus précisement: avec module quadratique Archimedien.

Applications

Quelques problème qui peut être résolu à l'aide des polynômes positifs:

- optimisation polynômiale $\quad (\inf\ f(x) \text{ t.q. } g_1(x) \geq 0, \ldots, g_m(x) \geq 0)$
- problème des moments $\quad$ (on cherche une mesure μ étant donnés ses moments d'ordre $\leq d$)
- problèmes de contrôle optimale
- mathématiques pour la finance, *option pricing*
- calcul d'équilibres de Nash
- calcul de l'enveloppe convexe d'ensembles

Conclusions

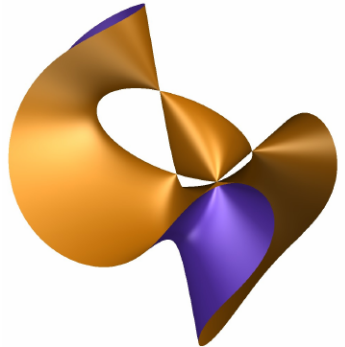
La théorie des polynômes positifs est un exemple parfait d'**intéraction** de plusieurs disciplines (même très éloignées) comme algèbre, calcul et l'optimisation.

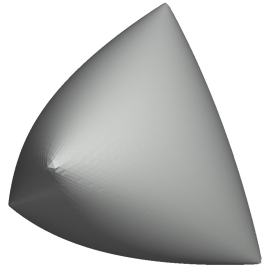
C'est un problème mathématique **abstrait**, qui a eu une évolution naturelle dans les **applications** des mathématiques.

Minkowski et Hilbert n'avaient vraisemblablement pas prévu que leur dialogue sur les formes positives aurait amené à parler, plus d'un siècle après, d'optimisation avec les polynômes (ou peut être si ?)

Vive les maths et l'info, et surtout, vive les polynômes !

Ensembles de certificats : Spectraèdres





$$\det \begin{bmatrix} 1 & \lambda & \mu \\ \lambda & 1 & \nu \\ \mu & \nu & 1 \end{bmatrix} = 0$$

$$\begin{bmatrix} 1 & \lambda & \mu \\ \lambda & 1 & \nu \\ \mu & \nu & 1 \end{bmatrix} \succeq 0$$