

Astérisque

A.-M. BERGÉ

J. MARTINET

F. SIGRIST

Une généralisation de l'algorithme de Voronoï pour les formes quadratiques

Astérisque, tome 209 (1992), p. 137-158

http://www.numdam.org/item?id=AST_1992__209__137_0

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

UNE GÉNÉRALISATION DE L'ALGORITHME DE VORONOÏ POUR LES FORMES QUADRATIQUES

par A-M. BERGÉ, J. MARTINET et F. SIGRIST

§ 1. **Introduction.** Soit n un entier > 0 . On note $\mathcal{Q}_n$ l'espace vectoriel des formes quadratiques sur $\mathbb{R}^n$ que l'on identifie à l'espace vectoriel Sym_n des matrices symétriques d'ordre n à coefficients réels, en associant à $M \in \text{Sym}_n$ la forme $Q(x) = {}^t X M X$ où, pour $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$, X désigne la matrice-colonne de composantes $x_1, x_2, \dots, x_n$ et la notation ${}^t A$ désigne la transposée de la matrice A . Pour une forme Q définie positive, on pose $m(Q) = \min_{x \in \mathbb{Z}^n \setminus \{0\}} Q(x)$ (le *minimum* de Q) et $S(Q) = \{x \in \mathbb{Z}^n \mid Q(x) = m(Q)\}$ (ensemble des *vecteurs minimaux* de Q), et l'on note $\det(Q)$ le déterminant $\det(M)$ de la matrice correspondant à Q (le *discriminant* de Q). L'*invariant d'Hermite* de Q est $\gamma_n(Q) = m(Q)(\det(Q))^{-1/n}$, et la *constante d'Hermite* pour la dimension n est $\gamma_n = \sup_Q \gamma_n(Q)$.

Afin de calculer la constante d'Hermite, Korkine et Zolotareff ont introduit la notion de *forme extrême* (forme qui réalise un maximum local de l'invariant d'Hermite) et démontré le résultat suivant ([K-Z]) :

1.1. Théorème (KORKINE ET ZOLOTAREFF, 1877). *Si Q est une forme extrême, les formes de matrices $Y {}^t Y$, $Y \in S(Q)$ engendrent $\mathcal{Q}_n$. (En particulier, Q possède au moins $\frac{n(n+1)}{2}$ couples de vecteurs minimaux.)*

Les formes vérifiant cette propriété ont été appelées par la suite *formes parfaites* par Voronoï, qui a notamment démontré qu'elles sont en nombre fini à proportionnalité et équivalence sous $\text{Gl}_n(\mathbb{Z})$ près. C'est la notion de forme parfaite plutôt que celle de forme extrême qui est importante dans les applications.

mots-clés : Formes quadratiques réelles, Formes parfaites, Réseaux parfaits.

[Noter que, lorsque Y parcourt les vecteurs-colonnes à n composantes, les matrices $Y^t Y$ parcourent l'ensemble des matrices positives de rang ≤ 1 de Sym_n , alors que ${}^t Y Y \in \mathbb{R}$ est le carré de la norme de Y .]

Korkine et Zolotareff, à l'aide de méthodes combinatoires, ont classé les formes parfaites jusqu'à la dimension 5, trouvant ainsi la valeur de γ_5 ([K-Z], 1877). L'étude des formes parfaites a été reprise 30 ans plus tard par Voronoï (dans [V], paru en 1908), qui a introduit une méthode entièrement nouvelle qui sera décrite en détail au § suivant. Indiquons simplement ici qu'il associe à toute forme parfaite Q de dimension $n \geq 2$ et de minimum m donné un cône polyédral d'intérieur non vide de $\mathcal{Q}_n$ et à toute face de ce cône une forme parfaite dite contiguë à Q , et qu'il démontre que le graphe de contiguïté ainsi obtenu est connexe. La relation de contiguïté étant compatible à l'équivalence, l'ensemble des classes de formes parfaites de minimum donné se trouve muni d'une structure de graphe qui est fini et connexe, ce qui entraîne la validité du procédé de calcul suivant :

1.2. Algorithme (VORONOÏ, 1908)

1. Choisir une forme parfaite Q_0 pour la dimension n .
2. Déterminer ses formes contiguës $Q_1, \dots, Q_r$.
3. Supprimer de la liste toute forme équivalente à une forme déjà rencontrée.
4. Terminer si aucune forme nouvelle n'a été conservée.
5. Sinon, faire la liste de toutes les formes contiguës à l'une des formes nouvelles et aller en 3.

À l'aide de cet algorithme, Voronoï ([V]) a vérifié les résultats de Korkine et Zolotareff pour les dimensions ≤ 5 . Son article indique qu'il a également commencé l'étude de la dimension 6 (et il y annonce aussi diverses autres recherches qu'il serait peut-être intéressant de reprendre). Son décès survenu en 1908 l'a empêché de poursuivre son programme. Le cas de la dimension 6 a été résolu un demi-siècle plus tard par Barnes ([Ba]), et celui de la dimension 7 vient d'être résolu par Jaquet ([J]). Cette dernière étude a nécessité des calculs considérables sur ordinateur, et il ne semble pas possible de traiter la dimension 8 selon les mêmes procédés.

Cela suggère de restreindre l'étude de l'invariant d'Hermite à certaines familles de formes quadratiques pour lesquelles on peut développer un algorithme analogue dans un sous-espace $\mathcal{T}$ de $\mathcal{Q}_n$ de dimension inférieure. Le paragraphe 2 est consacré à la description de cet algorithme. Voici deux exemples qui seront étudiés avec quelques détails dans cet article :

1.3. Exemple. Étant donnée une représentation intégrale $\rho : G \rightarrow \text{Gl}_n(\mathbb{Z})$ d'un groupe fini G , on étudie l'ensemble $\mathcal{Q}_\rho$ des formes quadratiques définies positives invariantes par $\rho(G)$; dans ce cas, on peut prendre pour $\mathcal{T}$ l'espace de toutes les formes quadratiques invariantes par $\rho(G)$.

Cet exemple est étudié en détail aux §§ 3, où est justifié le choix fait pour $\mathcal{T}$ en même temps qu'est établi le lien avec la notion de G -réseau développée dans [B-M], et 4, consacré aux résultats effectifs obtenus à l'aide de l'algorithme de Voronoï.

1.4. Exemple. Soit $Q_0 = Q_0(x_1, x_2, \dots, x_r)$ une forme quadratique définie positive à $r < n$ variables. On étudie les formes quadratiques définies positives $Q \in \mathcal{Q}_n$ de même minimum que Q_0 et telles que $Q(x_1, x_2, \dots, x_r, 0, 0, \dots, 0) = Q_0(x_1, x_2, \dots, x_r)$. On se place alors dans l'espace $\mathcal{T}$ des formes $Q \in \mathcal{Q}_n$ telles que $Q(x_1, \dots, x_r, 0, \dots, 0) = 0$. Pour plus de détails, se reporter au § 5.

Le problème de développer un algorithme de Voronoï dans le cas des G -réseaux (exemple 1.3 ci-dessus) est posé dans [B-M]. Il a été résolu indépendamment de nous par Joseph Oesterlé, que nous remercions par ailleurs pour les discussions fructueuses que nous avons eues avec lui.

§ 2. Nouvel algorithme de Voronoï. On munit Sym_n du produit scalaire $\langle A, B \rangle = \text{Tr}(AB)$. On en déduit un produit scalaire sur $\mathcal{Q}_n$, et par restriction sur tous les sous-espaces de Sym_n et de $\mathcal{Q}_n$. Pour $x \in \mathbb{R}^n$, on note P_x ou P_X la forme de matrice $X^t X \in \text{Sym}_n$. On a alors, pour $x \in \mathbb{R}^n$ et $Q \in \mathcal{Q}_n$, $Q(x) = \langle Q, P_x \rangle = \langle A, P_x \rangle$, où A est la matrice représentant la forme quadratique Q .

2.1. Définition. Soit $\mathcal{T}$ un sous-espace vectoriel de $\mathcal{Q}_n$.

- (1) Pour tout $x \in \mathbb{R}^n$ représenté par la matrice-colonne X , on note Ω_x (ou Ω_X) la projection orthogonale de $P_x = P_X$ sur $\mathcal{T}$.
- (2) On dit qu'une forme quadratique définie positive Q est $\mathcal{T}$ -parfaite (ou que la matrice de Q est $\mathcal{T}$ -parfaite) si les matrices Ω_x engendrent $\mathcal{T}$ tout entier lorsque x décrit l'ensemble $S(Q)$ des vecteurs minimaux de Q .

Si $\mathcal{T}'$ est un sous-espace de $\mathcal{T}$, toute forme $\mathcal{T}$ -parfaite est $\mathcal{T}'$ -parfaite. Lorsque $\mathcal{T} = \mathcal{Q}_n$, on retrouve la notion de forme parfaite introduite par Voronoï. On montre facilement que les vecteurs minimaux d'une forme parfaite engendrent $\mathbb{R}^n$. Nous nous restreindrons aux sous-espaces $\mathcal{T}$ vérifiant une propriété analogue :

2.2. Hypothèse. Désormais, $\mathcal{T}$ désigne un sous-espace vectoriel de $\mathcal{Q}_n$

vérifiant la propriété suivante : les vecteurs minimaux des formes $\mathcal{T}$ -parfaites engendrent $\mathbb{R}^n$.

La proposition suivante donne d'autres expressions de cette condition :

2.3. Proposition. Soit Q une forme quadratique définie positive. Les conditions suivantes sont équivalentes :

- (1) Il existe des coefficients positifs $\lambda_x, x \in S(Q)$ tels que la forme quadratique $\sum_{x \in S} \lambda_x P_x$ soit définie positive.
- (2) Pour toute famille de coefficients positifs $\lambda_x, x \in S$, la forme quadratique $\sum_{x \in S} \lambda_x P_x$ est définie positive.
- (3) $S(Q)$ engendre $\mathbb{R}^n$.

Démonstration. Quel que soit le vecteur $u \in \mathbb{R}^n$ et les coefficients $\lambda_x > 0$, on a

$$\sum_{x \in S(Q)} \lambda_x \langle P_x, P_u \rangle = \sum_{x \in S(Q)} \lambda_x (x \cdot u)^2 \geq 0,$$

et l'égalité a lieu si et seulement si u est orthogonal à x pour tout $x \in S(Q)$ (l'espace $\mathbb{R}^n$ étant muni de son produit scalaire canonique). On en déduit tout de suite les équivalences de (1) et (3) d'une part et de (2) et (3) d'autre part, **c.q.f.d.**

2.4. Définition. Soit Q une forme quadratique définie positive. Le $\mathcal{T}$ -domaine de Voronoï $\mathcal{D}_Q$ de Q est l'enveloppe convexe dans $\mathcal{T}$ des demi-droites fermées portant les formes Ω_x pour $x \in S(Q)$. Si Q a pour matrice A , on écrit aussi $\mathcal{D}_A$ au-lieu de $\mathcal{D}_Q$.

Lorsque $\mathcal{T} = \mathcal{Q}_n$, on retrouve la notion de domaine de Q introduite par Voronoï. (En fait, le $\mathcal{T}$ -domaine de Q est la projection sur $\mathcal{T}$ du domaine classique).

On a

$$\mathcal{D}_Q = \mathcal{D}_A = \left\{ \sum_{x \in S(Q)} \lambda_x \Omega_x \mid \lambda_x \geq 0 \right\},$$

et l'intérieur du $\mathcal{T}$ -domaine de Voronoï de Q est

$$\text{Int}(\mathcal{D}_Q) = \left\{ \sum_{x \in S(Q)} \lambda_x \Omega_x \mid \lambda_x > 0 \right\}.$$

Dire que Q est $\mathcal{T}$ -parfaite revient à dire que $\mathcal{D}_Q$ est d'intérieur non vide dans $\mathcal{T}$.