ANNALES DE L'INSTITUT FOURIER

DAVID-OLIVIER JAQUET-CHIFFELLE

Énumération complète des classes de formes parfaites en dimension 7

Annales de l'institut Fourier, tome 43, n° 1 (1993), p. 21-55

<http://www.numdam.org/item?id=AIF_1993__43_1_21_0>

© Annales de l'institut Fourier, 1993, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) 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/

Ann. Inst. Fourier, Grenoble
43, 1 (1993), 21-55

ÉNUMÉRATION COMPLÈTE DES CLASSES DE FORMES PARFAITES EN DIMENSION 7

par David-Olivier JAQUET-CHIFFELLE

0. Introduction.

La classification des formes parfaites en dimension inférieure à sept est un problème résolu depuis plus de trente ans. En 1831 déjà, Gauss montre que le réseau cubique à faces centrées est l'unique réseau extrême en dimension trois. Dans cette dimension, toute forme parfaite est équivalente à A_3 ; il n'existe donc qu'une seule classe de formes parfaites et ces formes sont absolument extrêmes. Pour les dimensions quatre et cinq, il faut attendre les travaux de Korkine et Zolotareff en 1877. En dimension quatre, on observe deux classes de formes parfaites (A_4 et D_4). En dimension cinq, leur nombre s'élève à trois. Quatre-vingts années plus tard, en 1957, Barnes démontre qu'il n'y a que sept classes de formes parfaites à six variables, dont une qui n'est pas extrême, conformément à ce que pensait Voronoï. A la fin de son article, Barnes prévoit que ses méthodes ne permettront certainement pas de traiter la dimension sept, vu la complexité du problème [Ba3].

La démonstration de Barnes se base sur le seul algorithme général qui garantit l'énumération complète des classes de formes parfaites en dimension n, à savoir le fameux algorithme de Voronoï [Vo1]. Sa complexité croît si rapidement en fonction de la dimension, que seule l'utilisation

Mots-Clés : Théorie des nombres – Théorie des graphes – Algorithme de Voronoï– Formes quadratiques réelles – Formes parfaites, extrêmes – Réseaux parfaits, extrêmes – Domaines de Voronoï– Enveloppe convexe – Identification des réseaux – Empilements de sphères.
Classification A.M.S. : 11E99.

d'ordinateurs permettait d'espérer pouvoir appliquer cet algorithme à la dimension sept.

En 1963, Scott tente de traiter certaines formes, en dimension sept, à l'aide de méthodes semblables à celles de Barnes, afin d'appliquer l'algorithme de Voronoï [Sc1]. Il y réussit partiellement, mais ses résultats contiennent des erreurs[(1)]. Jusqu'en 1971, on ne connaît que vingt-deux classes de formes parfaites à sept variables. Les travaux de Stacey permettent d'en découvrir onze nouvelles. Ces travaux sont basés sur des théorèmes de Watson. En fait, Stacey génère un grand nombre de formes parfaites. Mais elle n'arrive pas à décider si deux formes données sont équivalentes ou non. Pour effectuer un tri, elle considère un système de trois invariants ; lorsque deux formes coïncident sur ces invariants, elle n'en retient qu'une.

La liste obtenue par Stacey fut considérée comme très vraisemblablement exhaustive. Mais rien ne permettait d'exclure, a priori, que deux formes parfaites non équivalentes coïncident sur ce système de trois invariants. Dès lors, le problème fut de montrer que cette liste de trente-trois formes était effectivement exhaustive.

Dans un article paru en 1988, Conway et Sloane affirment que seules vingt-sept de ces formes ont été traitées dans l'optique de Voronoï et ils qualifient ces résultats d'incertains [CS2]. Mes programmes, écrits en LISP, m'ont permis de traiter dans un premier temps trente-deux de ces trente-trois formes (pour D_7, cf [JS1]). Une version plus complexe, que j'ai développée ultérieurement, a rendu possible le traitement de la dernière, à savoir E_7.

Mes travaux, comme ceux de Barnes, se basent sur l'algorithme de Voronoï. Par contre, les méthodes utilisées pour caractériser les faces d'un domaine sont entièrement nouvelles.

Voronoï, dans son étude générale de D_n, emploie certaines astuces très particulières qui permettent d'exhiber une liste suffisante de faces. De même, les travaux de Barnes contiennent très souvent des astuces de ce genre qui, dans un certain sens, localisent le problème et, par conséquent, le simplifient. Dans sa version la plus complexe, mon programme automatise, d'un certain point de vue, cette découverte d'astuces particulières.

---

(1) Dans sa thèse, Scott décrit les orbites de faces de certains domaines associés à des formes parfaites à sept variables. Les erreurs rencontrées sont les suivantes :
- les faces W_{13} et W_{14} du domaine associé à ϕ_1 sont équivalentes.
- les facettes W_{12}, W_{20} et W_{26} du domaine associé à ϕ_4 ne sont pas des faces du domaine. En effet, bien qu'elles contiennent vingt-sept arêtes, elles sont de codimension 2.

Ces mêmes programmes, appliqués aux dimensions inférieures à sept, m'ont permis, entre autres, de confirmer très rapidement les résultats de Barnes et de donner une description plus détaillée de la manière dont s'imbriquent les domaines de Voronoï. En particulier – et ceci est un résultat nouveau – le domaine associé à E_6 possède exactement 38 124 faces qui se répartissent, conformément aux résultats de Barnes, en 11 orbites sous l'action du groupe des automorphismes de E_6.

L'ordinateur utilisé, un VAX 8530, a travaillé pendant plus de cent vingt jours "CPU" pour traiter complètement la dimension sept. Les résultats de ces calculs démontrent le théorème suivant :

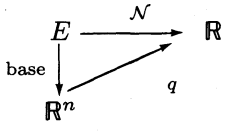
THÉORÈME. — *Il n'existe que trente-trois classes de formes parfaites à sept variables.*

On notera, au passage, que ces calculs ont permis de décrire complètement le domaine associé à E_7 ; ce domaine possède exactement 79 900 912 faces qui se répartissent en 157 orbites sous l'action du groupe des automorphismes de E_7.

L'article qui suit condense les développements mathématiques et les algorithmes contenus dans ma thèse de doctorat (Université de Neuchâtel).

2. Définitions.

Soit E, un espace vectoriel réel de dimension n, muni d'un produit scalaire $< \cdot | \cdot >$ et $q : \mathbb{R}^n \to \mathbb{R}$, une forme quadratique définie positive. A isométrie près, il existe une unique base de E pour laquelle q soit l'application "norme au carré", c'est-à-dire pour laquelle le diagramme suivant soit commutatif :



où $\mathcal{N}(v) =< v|v >$.

Figure 1

Si Q représente la matrice de Gram de cette base, $\forall x \in \mathbb{R}^n$, $q(x) = x^t Q x$; on dira que le réseau engendré par les vecteurs de cette base est un réseau associé à q.

Si une autre base de E engendre le même réseau, la matrice S de changement de base appartient à $GL_n(\mathbb{Z})$.

Deux réseaux sont équivalents s'ils sont semblables (équivalence "naturelle"). Les réseaux de E associés à q étant isométriques sont donc équivalents. On en déduit une relation d'équivalence entre formes quadratiques définies positives, compatible avec l'équivalence entre réseaux : deux formes q et q' sont équivalentes s'il existe $S \in GL_n(\mathbb{Z})$, telle que q soit positivement proportionnelle à $q' \circ S$.

Ainsi, on obtient une bijection entre classes de formes quadratiques définies positives et classes de réseaux.

Par définition, le *minimum de* q (et de Q) est :

$$\min q = \min q(x) = \min x^t Q x = \min Q \text{ où } x \in \mathbb{Z}^n, x \neq 0.$$

Les paires de vecteurs $\pm v \in \mathbb{Z}^n$ vérifiant $q(v) = \min q$ sont appelées *paires de vecteurs minimaux* de q (et de Q). Géométriquement, les vecteurs minimaux de q correspondent aux points d'un réseau associé à q, les plus proches de l'origine.

Le nombre $\operatorname{disc} q = \det Q$ est appelé *discriminant de* q. La racine de $\operatorname{disc} q$ est égale au volume d'une maille d'un réseau associé à q.

On définit l'application suivante, dite *invariant d'Hermite* :

$$\mu : q \mapsto \mu(q) = \frac{\min q}{\sqrt[n]{\operatorname{disc} q}}.$$

La fonction μ est invariante sur les classes de formes quadratiques définies positives ; elle est directement liée à la densité des empilements de sphères associés aux réseaux.

On définit γ_n, appelée *constante d'Hermite*, par $\gamma_n = \sup \mu(q)$, lorsque q varie dans l'ensemble des formes quadratiques définies positives à n variables. On démontre que μ atteint ses maxima ; en particulier, la valeur de γ_n est atteinte.

Les formes quadratiques définies positives correspondant aux maxima locaux de la fonction μ sont dites *extrêmes*, celles qui vérifient $\mu(q) = \gamma_n$, *absolument extrêmes*.

Une forme quadratique définie positive est dite *parfaite* si elle est entièrement caractérisée par la valeur de son minimum et l'ensemble de ses vecteurs minimaux.

Considérons maintenant l'espace des formes quadratiques, définies ou non, à n variables. Cet espace vectoriel est isomorphe à $\mathrm{Sym}_n(\mathbb{R})$ qui,

muni du produit scalaire $(X, Y) \mapsto \text{trace}\,(XY)$, est un espace euclidien de dimension $N = \dfrac{n(n+1)}{2}$: l'espace de Voronoï, noté $\mathcal{V}$.

Soit q une forme parfaite, indiçons ses paires de vecteurs minimaux : $\pm v_k, k = 1, ..., s$. A chaque paire $\pm v_k$ correspond une forme quadratique positive $q_k(x)$: $q_k : x \mapsto q_k(x) = (v_k^t x)^2$, et donc un point $v_k v_k^t$ dans l'espace de Voronoï. Appelons d_k la demi-droite, issue de l'origine et passant par $v_k v_k^t$. L'enveloppe convexe des d_k est un cône convexe appelé *domaine de Voronoï* associé à q (et à Q).

On appelle *face* du domaine tout cône convexe de codimension 1 obtenu en intersectant le domaine avec un de ses hyperplans d'appui.

Plus généralement, une *d-face* sera un cône convexe de dimension $d \geq 1$ obtenu en intersectant des faces du domaine. Les *1-faces* sont les arêtes du domaine.

Si $q(x) = x^t Q x$, on définit q^{ad} par $q^{\text{ad}} : x \mapsto q^{\text{ad}}(x) = x^t Q^{\text{ad}} x$ où Q^{ad} est la matrice adjointe de Q. On dira que q est *eutactique* si q^{ad} peut s'exprimer comme combinaison linéaire à coefficients strictement positifs des q_k. Géométriquement, si q est parfaite, cela revient à demander que Q^{ad} soit un point intérieur du domaine associé à q.

Voronoï démontre un critère, maintenant classique, pour les formes extrêmes : *une forme quadratique définie positive est extrême si et seulement si elle est parfaite et eutactique.*

3. La fonction d'Hermite μ.

La recherche des réseaux les plus denses en dimension n revient à caractériser les maxima de la fonction μ. Pour n fixé, la fonction μ est bornée; Minkowski a montré, par exemple, que pour n donné supérieur à 1, γ_n est inférieur à n. Il emploie pour cela des méthodes liées à la géométrie des nombres.

On démontre que, modulo les homothéties, les maxima de μ sont isolés et, qu'à équivalence près, il n'y a qu'un nombre fini de formes extrêmes. Historiquement, c'est la recherche de ces classes de formes extrêmes qui a introduit la notion de formes parfaites. La classification des formes extrêmes fut ramenée à la classification des formes parfaites. On ne connaît les valeurs

exactes de γ_n que pour $n \leq 8$:

$$\gamma_1 = 1 \quad \gamma_2 = \sqrt{\frac{4}{3}} \quad \gamma_3 = \sqrt[3]{2} \quad \gamma_4 = \sqrt{2}$$
$$\gamma_5 = \sqrt[5]{8} \quad \gamma_6 = \sqrt[6]{\frac{64}{3}} \quad \gamma_7 = \sqrt[7]{64} \quad \gamma_8 = 2.$$

Les valeurs de γ_6, γ_7 et γ_8 furent déterminées par Blichfeldt, voici près de soixante ans : γ_6 en 1925, γ_7 en 1929 et γ_8 en 1935 [Bl1], [Bl2], [Bl3]. En 1944, Mordell montra à l'aide de l'inégalité qui porte son nom que, de la connaissance de γ_7, on peut déduire celle de γ_8 [Mo1].

En 1966, Watson annonça qu'il était capable de vérifier les calculs de Blichfeldt... et démontra l'unicité des formes absolument extrêmes en dimension 6, 7 et 8 [Wa1].

Plus récemment, en 1980, Vetchinkin confirma les résultats de Blichfeldt et de Watson dans un article très détaillé [Ve1].

L'énumération complète des classes de formes parfaites à sept variables a pour corollaire une confirmation immédiate des valeurs de γ_7 et γ_8.

4. Généralités sur les convexes.

4.1. Propriétés fondamentales.

Soit E un espace euclidien et $l_1, ..., l_t$ des vecteurs de E. On définit $\mathcal{C}$ – cône convexe de E – par $\mathcal{C} = \{x \in E \mid l_i \cdot x \geq 0, i = 1, ..., t\}$.

THÉORÈME 1. — *$\mathcal{C}$ est une variété de dimension maximale dans E si et seulement si les l_i sont linéairement positivement indépendants, c'est-à-dire si $\sum_{i=1}^{t} \rho_i l_i = 0$, avec $\rho_i \geq 0$, implique $\rho_i = 0$ pour tout i.*

THÉORÈME 2. — *Supposons $\mathcal{C}$ de dimension maximale; après élimination éventuelle des l_i pouvant s'exprimer comme combinaison linéaire positive des autres l_j ($j \neq i$), ceux qui restent définissent les hyperplans d'appui de $\mathcal{C}$ qui contiennent les faces de $\mathcal{C}$, cônes convexes de codimension 1.*

THÉORÈME 3. — *Supposons $\mathcal{C}$ de dimension maximale. Si ($l_i \cdot x = 0 \; \forall i \Rightarrow x = 0$), alors $\mathcal{C}$ est un cône convexe saillant; il possède des arêtes (représentées par a_1, a_2, ..., a_s), et tout point de $\mathcal{C}$ peut s'exprimer comme*

combinaison linéaire positive des a_k, *c'est-à-dire :* $\mathcal{C} = \left\{ x \in E \mid x = \sum_{k=1}^{s} \rho_k a_k, \rho_k \geq 0 \right\}$.

On trouvera dans la littérature diverses démonstrations de ces trois théorèmes classiques à propos des cônes convexes. Dans ce qui suit, on supposera toujours que $\mathcal{C}$ satisfait les hypothèses des théorèmes 2 et 3.

Si π, d'équation $l \cdot x = 0$, contient une face de $\mathcal{C}$, le théorème 3 garantit que π est l'enveloppe linéaire des représentants des arêtes de $\mathcal{C}$ qu'il contient. Il existe donc J, un ensemble d'indices, qui dépend de π, tel que les conditions suivantes $(*)$ définissent l à un facteur positif près :

$(*)$ $l \cdot a_j = 0$ si $j \in J$ et $l \cdot a_j \geq 0$ sinon.

Inversement, s'il existe J, un ensemble d'indices tel que les conditions $(*)$ définissent l à un facteur positif près, l'hyperplan d'équation $l \cdot x = 0$ est un hyperplan d'appui qui contient une face de $\mathcal{C}$.

En effet, en appliquant le théorème 3, on constate que pour tout x appartenant à $\mathcal{C}$, $l \cdot x \geq 0$; d'autre part, il est clair, sous ces conditions, que l'ensemble des $x \in \mathcal{C}$ vérifiant $l \cdot x = 0$ est de dimension maximale dans cet hyperplan.

On appellera *facette* d'un cône convexe saillant de dimension maximale toute face ou d-face de ce cône.

Soit F_I, une facette de $\mathcal{C}$: $F_I = \cap F_i$ où i parcourt l'ensemble d'indices I. Appelons E_I le plus petit sous-espace de E contenant F_I. Dans E_I, F_I est un cône de dimension maximale. Cela a donc un sens de parler des facettes de F_I.

On montre facilement que $F_I \subset E_I$ satisfait les hypothèses du théorème 3 et que :

LEMME 1. — *Toute facette de* F_I *est une facette de* $\mathcal{C}$.

LEMME 2. — *Toute facette de* $\mathcal{C}$ *strictement contenue dans* F_I *est une facette de* F_I.

COROLLAIRE. — *Toute facette de* $\mathcal{C}$ *est entièrement caractérisée par la liste des arêtes de* $\mathcal{C}$ *qu'elle contient. Les arêtes d'une telle facette sont exactement les arêtes de* $\mathcal{C}$ *qu'elle contient ; elle en est l'enveloppe convexe.*

Soit a, un vecteur représentant une arête de $\mathcal{C}$; il existe I, un ensemble d'indices tel que : $\{x \in E \mid x = \rho a, \rho \geq 0\} = \cap F_i$ avec $i \in I$. Cela revient

à dire que les conditions $l_i \cdot x = 0$ si $i \in I$ et $l_j \cdot x \geq 0$ $\forall j$ définissent le vecteur a à un facteur positif près.

On en déduit le lemme suivant :

LEMME 3. — *Un représentant d'une arête de $\mathcal{C}$ ne peut jamais s'exprimer comme combinaison linéaire positive des représentants des autres arêtes de $\mathcal{C}$.*

Finalement, en utilisant le théorème 3, on montrera que :

LEMME 4. — *Tout point intérieur de $\mathcal{C}$ (resp. d'une facette de $\mathcal{C}$) peut s'exprimer comme combinaison linéaire strictement positive des représentants des arêtes de $\mathcal{C}$ (resp. de cette facette).*

4.2. Relèvement d'un cône saillant.

4.2.1. Définitions et propriétés fondamentales.

Considérons un cône convexe saillant $\mathcal{C}$, de dimension d, dans un espace euclidien E de dimension s ($s \geq d$). On supposera $\mathcal{C}$ donné par $\mathbb{A} = \{a_1, a_2, ..., a_s\}$ où a_i est un vecteur représentant la $i^{\text{ème}}$ arête de $\mathcal{C}$. Après renumérotation éventuelle, on peut supposer $a_1, a_2, ..., a_d$ linéairement indépendants.

Notons E^d, l'enveloppe linéaire des a_i. E^d est un sous-espace de dimension d de l'espace euclidien E. Construisons, maintenant, une suite d'espaces euclidiens emboîtés $E^d \subset E^{d+1} \subset ... \subset E^s = E$, telle que E^k soit de dimension k et s'obtienne par adjonction à E^{k-1} d'un vecteur $e_k \perp E^{k-1}$.

Pour tout entier k, $d \leq k \leq s$, on définit l'application r^k :

$$r^k : \mathbb{A} \to E^k$$
$$a_i \mapsto a_i \text{ si } 1 \leq i \leq s+d-k;\ a_i + e_{s+d+1-i} \text{ si } i > s+d-k.$$

Pour simplifier les notations, posons $a_i^k = r^k(a_i)$ et $\mathbb{A}^k = r^k(\mathbb{A})$. Ainsi :

$$\mathbb{A}^d = \mathbb{A}$$
$$\mathbb{A}^{d+1} = \{a_1, a_2, ..., a_{s-1}, a_s + e_{d+1}\}$$
$$\mathbb{A}^{d+2} = \{a_1, a_2, ..., a_{s-1} + e_{d+2}, a_s + e_{d+1}\}$$
etc.
$$\mathbb{A}^s = \{a_1, a_2, ..., a_d, a_{d+1} + e_s, a_{d+2} + e_{s-1}, ..., a_{s-1} + e_{d+2}, a_s + e_{d+1}\}.$$

Dans E^k, définissons maintenant $\mathcal{C}^k$, l'enveloppe convexe des demi-droites issues de l'origine, caractérisées par les éléments de $\mathbb{A}^k$. Observons d'abord que les éléments de $\mathbb{A}^k$ sont linéairement positivement indépendants puisque les éléments de $\mathbb{A}$ le sont.

En s'inspirant de la démonstration de Voronoï qui, utilisant la notion de domaines corrélatifs, montre que les arêtes d'un domaine associé à une forme parfaite sont parmi les demi-droites dont on prend l'enveloppe convexe, on vérifiera sans peine que $\mathcal{C}^k$ est un cône convexe saillant dont les arêtes sont exactement caractérisées par les éléments de $\mathbb{A}^k$.

4.2.2. THÉORÈME FONDAMENTAL. — *Pour tout entier k, $d < k \leq s$, notons p^k la projection orthogonale de E^k sur E^d et π^k la projection orthogonale de E^k sur E^{k-1}. Par construction, $\pi^k(a_i^k) = a_i^{k-1}$ et $p^k(a_i^k) = a_i$. On en déduit que $p^k(\mathcal{C}^k) = \mathcal{C}, \pi^k(\mathcal{C}^k) = \mathcal{C}^{k-1}$ et $p^k \circ r^k =$ identité.*

THÉORÈME 4. — *Toute face de $\mathcal{C}^{k-1}$ est projection par π^k, soit d'une face de $\mathcal{C}^k$, soit de l'intersection de deux faces de $\mathcal{C}^k$.*

Démonstration. — Soit F', une face de $\mathcal{C}^{k-1}$. F' est une variété de dimension $k-2$. Considérons α', l'hyperplan d'appui dans E^{k-1} qui contient cette face et $\alpha = (\pi^k)^{-1}(\alpha')$, l'hyperplan dans E^k engendré par α' et e_k. Notons I, l'ensemble des indices des représentants des arêtes de $\mathcal{C}^{k-1}$ contenues dans F'. Par le corollaire des lemmes 1 et 2, ces arêtes sont les arêtes de F'.

Tous les points de $\mathcal{C}^k$ sont du même côté de α, puisque tous les points de $\mathcal{C}^{k-1}$ sont du même côté de α'.

Notons l_i, les vecteurs normaux aux hyperplans d'appui de $\mathcal{C}^k$, et l, un vecteur normal à α. On choisira le sens de l et celui des l_i de telle sorte que, pour tout x appartenant à $\mathcal{C}^k$, on ait $l_i \cdot x \geq 0$ et $l \cdot x \geq 0$.

La variété de E^k définie par $l_i \cdot x \geq 0, \forall i$ et $(-l) \cdot x \geq 0$ vit dans α. Par le théorème 1, il existe $\rho \geq 0$ et $\rho_i \geq 0$, non tous nuls, tels que : $\rho(-l) + \sum \rho_i l_i = 0$.

Comme les l_i sont linéairement positivement indépendants, ρ doit être non nul, et il existe au moins un ρ_i non nul. Après renumérotation éventuelle, on peut supposer $\rho_1 > 0$.

Donc, $l = \sum \frac{\rho_i}{\rho} l_i$ avec $\rho_1 > 0$.

Comme les $a_i^k, i \in I$, sont contenus dans α, $l \cdot a_i^k = 0$ si $i \in I$. Si $\rho_1 > 0$, on déduit de ce qui précède que $l_1 \cdot a_i^k = 0$ si $i \in I$. Cela signifie

que les $a_i^k, i \in I$, sont tous contenus dans la face F_1 et représentent donc des arêtes de cette face. Deux cas sont possibles :

Premier cas : un seul ρ_i est non nul, disons ρ_1.

Dans ce cas, l est positivement proportionnel à l_1. Toute arête de F_1 étant une arête de $\mathcal{C}^k$, elle se projette par π^k sur une arête de $\mathcal{C}^{k-1}$ contenue dans α', donc une arête de F'. Les arêtes de F' étant caractérisées par les $a_i^{k-1}, i \in I$, on en conclut que les $a_i^k, i \in I$, caractérisent toutes les arêtes de F_1. Par conséquent, par linéarité de π^k, $\pi^k(F_1) = F'$.

Second cas : un second ρ_i est non nul, disons ρ_2.

Notons F_1 et F_2, les faces correspondantes de $\mathcal{C}^k$, et posons $D = F_1 \cap F_2$; nous allons montrer que $\pi^k(D) = F'$.

D étant une facette de $\mathcal{C}^k$, il suffit de voir que les $a_i^k, i \in I$, caractérisent exactement les arêtes de D. Comme toute arête de $\mathcal{C}^k$ contenue dans F_1 et dans F_2 est une arête de D, les $a_i^k, i \in I$, caractérisent des arêtes de D. Reste à voir qu'il n'y en a pas d'autres.

A priori, D est un cône convexe de dimension inférieure ou égale à $k-2$. Mais comme α' est l'enveloppe linéaire des $a_i^{k-1}, i \in I$, la dimension de l'enveloppe linéaire des $a_i^k, i \in I$, doit être supérieure ou égale à $k-2$. Par conséquent, dans ce cas, elle vaut exactement $k-2$, et D est un cône convexe, de dimension $k-2$, contenu dans l'enveloppe linéaire des $a_i^k, i \in I$.

On en déduit que la projection par π^k de toute arête de D, non seulement est une arête de $\mathcal{C}^{k-1}$, mais est contenue dans α' ; c'est une arête de F'. Comme précédemment, les arêtes de F' étant caractérisées par les $a_i^{k-1}, i \in I$, on en conclut que les $a_i^k, i \in I$, caractérisent toutes les arêtes de D.

4.3. Faces voisines.

4.3.1. Définition et propriété fondamentale.

On dira que deux faces F_1 et F_2 de $\mathcal{C}$ sont *voisines* si leur intersection est une facette de codimension 2.

LEMME 5. — *Si D est une facette de $\mathcal{C}$ de codimension 2, seules exactement deux faces de $\mathcal{C}$ contiennent D.*

Démonstration. — Par construction, D est contenue au moins dans deux faces de $\mathcal{C}$.

Considérons U, l'enveloppe linéaire des éléments de D, et $U^{\perp}$, son complémentaire orthogonal. Par hypothèse, $U^{\perp}$ est de dimension 2, c'est un 2-plan.

Soit F_i, une face quelconque de $\mathcal{C}$ contenant D, τ_i, l'hyperplan d'appui correspondant à F_i, et l_i, un vecteur perpendiculaire à τ_i. Le sens de l_i est fixé par la condition $l_i \cdot x \geq 0, \forall x \in \mathcal{C}$.

Observons que $l_i \cdot x = 0, \forall x \in D$. Par conséquent, $l_i \cdot x = 0, \forall x \in U$ et $l_i \in U^{\perp}$.

Par le théorème 1, on sait que les l_i sont linéairement positivement indépendants. Par le théorème 2, on peut supposer qu'aucun l_i ne puisse s'exprimer comme combinaison linéaire positive des autres $l_j (j \neq i)$.

Dans un 2-plan, seul un ensemble de deux vecteurs, au plus, peut satisfaire simultanément ces deux conditions.

COROLLAIRES. — *Soit D, une facette de $\mathcal{C}$ de codimension 2. Notons F et F' les deux seules faces de $\mathcal{C}$ qui contiennent D ; par définition d'une facette de $\mathcal{C}$, on sait que D est exactement l'intersection de F et de F'.*

Aucune autre face de $\mathcal{C}$ ne peut contenir un point intérieur de D. En effet, si x est un point intérieur de D, il peut s'exprimer comme combinaison linéaire strictement positive des représentants des arêtes de D. Ainsi, toute face de $\mathcal{C}$ contenant x contient toutes les arêtes de D et, par conséquent, D tout entier.

4.3.2. Connexion.

On dira que deux faces F et F' de $\mathcal{C}$ sont *connectées* s'il existe une liste de faces de $\mathcal{C}$: $F_1 = F, F_2, ..., F_t = F'$ avec la propriété que F_j et F_{j+1} sont voisines $\forall j$.

Remarque : "être connecté" est une relation d'équivalence.

4.3.2.1. Théorème fondamental.

THÉORÈME 5. — *Deux faces de $\mathcal{C}$ sont toujours connectées pour peu que $\mathcal{C}$, en tant que variété, soit de dimension ≥ 2.*

Démonstration. — Posons $l = \sum_{i=1}^{s} l_i$ et considérons π, l'hyperplan affine d'équation $l \cdot x = \sum_{j=1}^{s} a_j$.

Le fait que $l \cdot a_j > 0$, $\forall j$, montre que toute arête de $\mathcal{C}$ coupe π en un point.

L'intersection de π et de $\mathcal{C}$ est donc un polyèdre $\mathcal{P}$ convexe, compact, d'intérieur non-vide, c'est-à-dire un polytope.

Les faces de $\mathcal{P}$ sont en bijection avec celles de $\mathcal{C}$. De plus, cette bijection est compatible avec la propriété "être voisines".

On conclut en utilisant le théorème bien connu qui affirme que les faces de $\mathcal{P}$ sont connectées [Be1].

4.3.2.2. Faces maximales.

Dans ce qui suit, on supposera que $\mathcal{C}$ est un cône convexe saillant possédant s arêtes.

On dira qu'une facette de $\mathcal{C}$ est *maximale* si seule une arête de $\mathcal{C}$ n'est pas contenue dans cette facette. Il est clair que toute facette maximale de $\mathcal{C}$ est une face de $\mathcal{C}$. On parlera donc de *face maximale*.

On appellera *taille* d'un cône convexe $\mathcal{C}$ (resp. d'une facette de $\mathcal{C}$) la différence entre le nombre d'arêtes contenues dans $\mathcal{C}$ (resp. dans cette facette de $\mathcal{C}$) et la dimension de $\mathcal{C}$ (resp. de cette facette de $\mathcal{C}$).

Si $\mathcal{C}$ possède s arêtes, $\mathcal{C}$ possède au plus s faces maximales. Si $s = \dim \mathcal{C}$, $\mathcal{C}$ possède exactement s faces qui sont toutes maximales. La réciproque est vraie; si $\mathcal{C}$ possède s faces maximales, $\mathcal{C}$ ne possède pas d'autres faces et $s = \dim \mathcal{C}$ (théorème 7).

THÉORÈME 6. — *Soit F une face maximale de $\mathcal{C}$.*

(i) *Elle est voisine de toutes les autres faces de $\mathcal{C}$.*

(ii) *Il y a bijection naturelle entre les faces de $\mathcal{C}$ différentes de F et les faces de F.*

(iii) *Cette bijection est compatible avec la relation "être voisine".*

(iv) *Cette bijection conserve la taille.*

(v) *Cette bijection conserve la propriété "être maximale".*

Démonstration. — Soit F', une face de $\mathcal{C}$ différente de F. Considérons $f' = F \cap F'$. f' est une facette de $\mathcal{C}$ contenue dans F'. Par le lemme 2, c'est une facette de F'. La seule arête de F' hors de f' étant celle de $\mathcal{C}$ qui n'est pas dans F, f' est une face maximale de F' et $\dim f' = (\dim F') - 1$.

(i) L'égalité dim $f' = (\dim F') - 1$ implique que F et F' sont voisines.

(ii) f' est une facette de $\mathcal{C}$ strictement contenue dans F. C'est une face de F. Le lemme 5 montre que l'application qui envoie F' sur $f' = F \cap F'$ crée une bijection entre l'ensemble des faces de $\mathcal{C}$ différentes de F et l'ensemble des faces de F.

(iii) Soit F_1 et F_2, deux faces de $\mathcal{C}$, différentes de F ; posons $f_1 = F \cap F_1$ et $f_2 = F \cap F_2$. $f_1 \cap f_2$ est une facette de $\mathcal{C}$ contenue dans $F_1 \cap F_2$; c'est une facette de $F_1 \cap F_2$. Vu qu'elle contient toutes les arêtes de $F_1 \cap F_2$, excepté celle de $\mathcal{C}$ qui n'est pas dans F, $f_1 \cap f_2$ est une face maximale de $F_1 \cap F_2$. En particulier, dim $(f_1 \cap f_2) =$ dim $(F_1 \cap F_2) - 1$. On déduit facilement de cette dernière égalité que f_1 et f_2 sont voisines si et seulement si F_1 et F_2 le sont.

(iv) D'une part, dim $f' =$ (dim F') $- 1$; d'autre part, F' possède exactement une arête de plus que f'. Donc, taille $f' =$ taille F'.

(v) Comme f' est toujours une face maximale de F' et F une face maximale de $\mathcal{C}$, f' est une face maximale de F si et seulement si F' est une face maximale de $\mathcal{C}$.

Conséquence : F possède exactement une face maximale de moins que $\mathcal{C}$.

On dira que deux faces F et F' de $\mathcal{C}$ sont *fortement connectées* s'il existe une liste de faces *non maximales* de $\mathcal{C}$: $F_1 = F$, $F_2, ..., F_t = F'$ avec la propriété que F_j et F_{j+1} sont voisines $\forall j$.

THÉORÈME 7. — *Soit $\mathcal{C}$, un cône convexe saillant de dimension supérieure ou égale à 3, possédant s arêtes. Notons $\psi(\mathcal{C})$, le nombre de ses faces maximales.*

(i) *Si $\psi(\mathcal{C}) >$ (dim $\mathcal{C}$) $- 3$, alors $\psi(\mathcal{C}) =$ dim$C = s$.*

(ii) *Si $\psi(\mathcal{C}) \leq$ (dim $\mathcal{C}$) $- 3$, alors $\mathcal{C}$ possède des faces non maximales et les faces non maximales de $\mathcal{C}$ sont fortement connectées.*

Démonstration (par induction sur la dimension de $\mathcal{C}$).

Ancrage : dim $\mathcal{C} = 3$:

(i) Si $\psi(\mathcal{C}) >$ (dim $\mathcal{C}$) $- 3 = 0$, $\mathcal{C}$ possède au moins une face maximale. Mais toutes les faces de $\mathcal{C}$ possèdent exactement deux arêtes. Donc $s = 3$, et les trois faces de $\mathcal{C}$ sont maximales.

(ii) Si $\psi(\mathcal{C}) \leq (\dim \mathcal{C}) - 3 = 0$, alors $\psi(\mathcal{C}) = 0$. Aucune face n'est maximale et on conclut en se rappelant que les faces de $\mathcal{C}$ sont toujours connectées.

Pas d'induction : dim $\mathcal{C} > 3$:

Si $\psi(\mathcal{C}) = 0$, on conclut comme pour l'ancrage (ii).

On supposera donc que $\mathcal{C}$ possède au moins une face F maximale. On a : $\psi(F) = \psi(\mathcal{C}) - 1$ et dim $F = (\dim \mathcal{C}) - 1 \geq 3$. Deux cas sont à envisager :

Cas 1 : $\psi(\mathcal{C}) > (\dim \mathcal{C}) - 3$; dans ce cas, $\psi(\mathcal{C}) - 1 > (\dim \mathcal{C}) - 3 - 1 \geq 0$, ce qui signifie $\psi(F) > (\dim F) - 3$.

En appliquant l'hypothèse d'induction à F, on obtient $\psi(F) =$ dim $F =$ (nombre d'arêtes dans F) $= s - 1$, puisque F est maximale. D'où l'égalité cherchée.

Cas 2 : $\psi(\mathcal{C}) \leq (\dim \mathcal{C}) - 3$; dans ce cas, $\psi(\mathcal{C}) - 1 \leq (\dim \mathcal{C}) - 3 - 1$, ce qui signifie $\psi(F) \leq (\dim F) - 3$.

En appliquant l'hypothèse d'induction à F, on obtient que F possède des faces non maximales et que ces faces non maximales sont fortement connectées. Les points (ii) et (v) du théorème 6 permettent alors de conclure que $\mathcal{C}$ possède des faces non maximales. Le point (iii) du théorème 6 montre qu'elles sont fortement connectées.

COROLLAIRES

1) *Si* $s >$ dim $\mathcal{C}$, *alors* $\psi(\mathcal{C}) \leq (\dim \mathcal{C}) - 3$ *et* $\mathcal{C}$ *possède des faces non maximales.*

Il suffit de remarquer que l'hypothèse $s >$ dim $\mathcal{C}$ *implique* dim $\mathcal{C} \geq 3$.

2) *Si* $s >$ dim $\mathcal{C}$, *on peut appliquer l'algorithme suivant pour énumérer toutes les faces de* $\mathcal{C}$:

a. Chercher une face non maximale de $\mathcal{C}$.

b. Calculer toutes ses faces voisines.

c. Mémoriser toutes les nouvelles faces.

d. Pour chaque nouvelle face non maximale, recommencer à partir du point b.

4.4. Graphe des faces d'un cône saillant.

Si $\mathcal{C}$ est un cône convexe saillant de dimension supérieure ou égale à deux, satisfaisant les hypothèses des théorèmes 2 et 3, la notion de faces voisines permet d'interpréter l'ensemble des faces de $\mathcal{C}$ comme un graphe localement fini; les faces jouent le rôle des sommets du graphe, les faces des faces, celui des arêtes.

Le lemme 5 montre que ce graphe est bien défini : chaque arête relie exactement deux sommets!

Le théorème 5 montre que ce graphe est connexe.

Le théorème 6 nous dit qu'à une face maximale de $\mathcal{C}$ correspond un sommet du graphe relié, par des arêtes, à tous les autres sommets. Lorsque le nombre d'arêtes de $\mathcal{C}$ est égal à la dimension de $\mathcal{C}$, le graphe des faces de $\mathcal{C}$ est complet.

5. Domaines de Voronoï.

5.1. Domaine associé à une forme parfaite.

On montre aisément qu'une forme est parfaite si et seulement si son domaine est de dimension maximale.

Le domaine d'une forme parfaite a été défini comme l'enveloppe convexe d'un ensemble bien déterminé de demi-droites. Nous allons voir que cet ensemble de demi-droites possède une propriété géométrique de minimalité, à savoir :

LEMME 6. — *Si l'on retire une demi-droite de cet ensemble, l'enveloppe convexe de celles qui restent est toujours modifiée.*

Démonstration. — Pour cela, remarquons d'abord que tout $a = vv^t, v \in \mathbb{R}^n$, fait un angle constant avec la matrice identité. On considère, bien entendu, la métrique définie par la trace. Cet angle satisfait $\cos\theta = \frac{1}{\sqrt{n}}$; en particulier, $\theta \in]0, \frac{\pi}{2}[$.

Considérons l'hyperplan d'équation trace $X = n$. Les intersections de cet hyperplan et des demi-droites dont on prend l'enveloppe convexe sont des points distincts, tous situés sur une sphère centrée en la matrice identité.

Ceci termine la démonstration.

On déduit facilement de ce qui précède le théorème suivant :

THÉORÈME 8. — *Le domaine de Voronoï associé à une forme parfaite est un cône convexe saillant.*

Les demi-droites dont on prend l'enveloppe convexe pour définir le domaine sont exactement les arêtes de ce domaine.

Remarque. — Voronoï, dans son article, montre que les arêtes du domaine sont parmi les demi-droites dont on prend l'enveloppe convexe [Vo1].

Contrairement aux apparences, il ne démontre pas que ces demi-droites sont exactement les arêtes du domaine. Il lui manque, en fait, le lemme 6 pour conclure.

5.2. Domaines voisins et formes voisines.

Soit q et q', deux formes parfaites, et leurs domaines $\mathcal{C}$ et $\mathcal{C}'$ dans l'espace de Voronoï. Si ces deux formes sont positivement proportionnelles, il est clair que $\mathcal{C} = \mathcal{C}'$. Sinon, Voronoï montre que l'intersection de ces deux domaines ne contient aucun point intérieur de $\mathcal{C}$ ou de $\mathcal{C}'$; mieux, si $\mathcal{C} \cap \mathcal{C}'$ contient un point intérieur d'une facette de $\mathcal{C}$, cette facette est aussi une facette de $\mathcal{C}'$. En particulier, si $\mathcal{C} \cap \mathcal{C}'$ contient un point intérieur d'une face de $\mathcal{C}$, cette face est commune à $\mathcal{C}$ et $\mathcal{C}'$. Dans ce cas, ces deux domaines doivent donc obligatoirement se situer de part et d'autre de l'hyperplan d'appui définissant la face commune. On dira que $\mathcal{C}$ et $\mathcal{C}'$ sont des domaines *voisins* et que les formes q et q' sont des formes *voisines*.

A chaque face de $\mathcal{C}$ correspond donc, au plus, un domaine voisin. Montrons qu'à chaque face de $\mathcal{C}$ correspond toujours un domaine voisin.

Soit Q, la matrice associée à q, F, une face de $\mathcal{C}$, et α, l'hyperplan d'appui d'équation $l \cdot x = 0$ associé à F. Le sens de l est fixé par la condition $l \cdot x \geq 0$, $\forall x \in \mathcal{C}$.

Montrons d'abord qu'il existe $u \in \mathbb{Z}^n$, tel que $\mathcal{C}$ et uu^t ne soient pas du même côté de α, ce qui revient à dire que la forme quadratique associée à l est indéfinie.

Pour cela, considérons L l'application linéaire associée à la matrice l. Observons qu'il existe une arête de F, caractérisée par $a = yy^t$ avec

$y \in \mathbb{Z}^n$, telle que $L(y)$ soit non nul. En effet, comme L est non nulle, son noyau est de dimension inférieure à n ; par conséquent, l'enveloppe linéaire, dans l'espace de Voronoï, des xx^t avec $x \in \mathrm{Ker}(L)$, est de dimension inférieure ou égale à $\frac{n(n-1)}{2}$. On conclut en remarquant que pour $n > 1$, $\frac{n(n-1)}{2} < \dim F = \frac{n(n+1)}{2} - 1$. Soit, donc, un vecteur $y \in \mathbb{Z}^n$, tel que :

(a) $L(y) = ly$ soit non nul et

(b) $y^t l y = 0$.

On choisira ensuite p et z dans $\mathbb{Z}^n$ satisfaisant :

(i) $p^t l p > 0$ (penser à une arête de $\mathcal{C}$ qui n'est pas dans F),

(ii) $z^t l y < 0$ (par exemple $z = -L(y)$).

On peut supposer que $p^t l y \leq 0$ (en remplaçant éventuellement p par $-p$) et que $z^t l z \geq 0$ (sinon, u=z est solution de notre problème).

Considérons finalement $w = \lambda p + z$. En remarquant que $w^t l y$ est négatif pour tout λ positif et que $w^t l w$ est positif dès que λ est suffisamment grand, on construit notre vecteur u en posant $u = (w^t l w) y - (w^t l y) w$ pour une certaine valeur entière de λ suffisamment grande. On vérifiera sans peine que si λ est assez grand, $u^t l u = -(w^t l w)(w^t l y) 2$ est négatif.

Si Q' est voisine de Q relativement à la face F, on peut supposer sans restreindre la généralité que $\min Q = \min Q'$. Du fait que l'enveloppe linéaire des représentants des arêtes de F est de codimension 1, on déduit que $Q' - Q$ est proportionnelle à l. Etudions par conséquent $Q(\theta) = Q + \theta l$, où θ est un nombre réel. Si $\theta < 0$, $\min Q(\theta) < \min Q$ et les vecteurs minimaux de Q associés aux arêtes de F ne sont plus vecteurs minimaux de $Q(\theta)$. Seul, le cas $\theta \geq 0$ reste donc intéressant.

Lorsque $\theta > 0$ est suffisamment petit, $\min Q(\theta) = \min Q$ et les vecteurs minimaux de $Q(\theta)$ sont exactement ceux correspondant aux arêtes de $\mathcal{C}$ contenues dans F. Considérons l'ensemble $\mathcal{R}$ des valeurs de $\theta \geq 0$ pour lesquelles $\min Q(\theta) = \min Q$.

L'existence d'un vecteur $u \in \mathbb{Z}^n$ satisfaisant $l \cdot (uu^t) < 0$ montre que, si θ est assez grand, $u^t Q(\theta) u < \min Q$. $\mathcal{R}$ est donc borné.

En observant que si $\min Q(\theta) = \min Q$, l'intervalle $[0, \theta]$ est entièrement contenu dans $\mathcal{R}$, on conclut que $\mathcal{R}$ est lui-même un intervalle.

La continuité de $\min Q(\theta)$ montre qu'il est fermé.

$\mathcal{R}$ est donc de la forme $[0, \rho]$ pour un certain $\rho > 0$.

Il est facile de voir que l'ensemble des valeurs de θ dans $\mathcal{R}$, pour lesquelles les vecteurs minimaux de $Q(\theta)$ sont exactement ceux correspondant aux arêtes de F, est un ouvert ; c'est même l'intérieur de $\mathcal{R}$. Par conséquent, la forme $Q' = Q + \rho l$ possède au moins un vecteur minimal supplémentaire. L'arête correspondante, n'appartenant pas à F, doit être extérieure à α. Le domaine associé à Q' est alors de dimension maximale dans l'espace de Voronoï. La forme Q' est parfaite ; elle est la voisine de Q relativement à la face F.

Soit v, un vecteur minimal de Q' qui n'est pas minimal pour Q. En observant que pour $\theta \geq \dfrac{v^t Q v}{-v^t l v}$, la forme $Q(\theta)$ n'est plus définie positive, on montre l'existence d'une valeur limite R pour θ, telle que $Q(\theta)$ soit définie positive si θ appartient à l'intervalle $[0, R[$, et $Q(\theta)$ soit indéfinie si θ est supérieur à R.

Le graphe de $\min Q(\theta)$ sur l'intervalle $[0, R[$ est une courbe continue, concave, composée de segments :

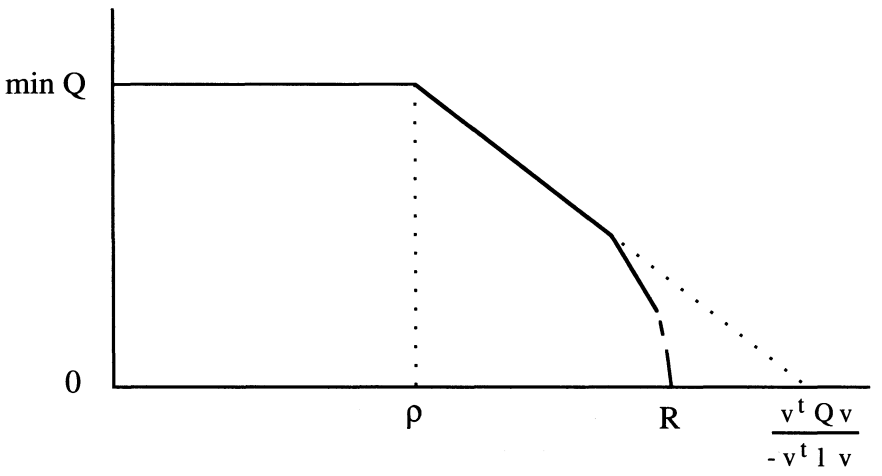


Figure 2

A ce stade, il est important de remarquer que, bien qu'une face d'un domaine $\mathcal{C}$ n'appartienne qu'à un seul autre domaine $\mathcal{C}'$, l'hyperplan α qui contient F peut contenir des faces d'autres domaines. Ainsi, le même hyperplan α peut être hyperplan d'appui de plusieurs domaines. La matrice l normale à α ne caractérise donc pas, en général, une unique face.

6. Graphe de Voronoï.

La notion de domaines voisins permet d'interpréter l'ensemble des domaines associés aux formes parfaites comme un graphe localement fini ; les domaines jouent le rôle des sommets du graphe, les faces des domaines celui des arêtes. Nous appellerons ce graphe, le *graphe de Voronoï.*

Nous allons montrer que le graphe de Voronoï est connexe. La démonstration est essentiellement basée sur le lemme suivant :

LEMME 7. — *Soit f, la matrice d'une forme quadratique définie positive et β, un nombre réel positif. Il n'existe au plus qu'un nombre fini de matrices A associées à des formes parfaites de minimum 1 et vérifiant $f \cdot A \leq \beta$.*

Démonstration. — Comme A est définie positive, il existe une matrice $S \in GL_n(\mathbb{R})$, telle que $A = S^t S$. Appelons l_k le vecteur dont les composantes sont celles de la k$^{\text{ème}}$ ligne de S. On montre facilement que $f \cdot A = \sum_{k=1}^{n} l_k^t f l_k$. f étant définie positive, chacun des termes $l_k^t f l_k$ doit être strictement inférieur à β, et la norme de S est bornée supérieurement par une constante qui ne dépend que de f.

La relation d'Hermite $\mu(A) \leq \gamma_n$ montre que le déterminant de S ne peut devenir arbitrairement petit. Ainsi, par Cramer, la norme de S^{-1} est aussi bornée supérieurement par une constante qui ne dépend que de f. On en déduit qu'en valeur absolue, les composantes des vecteurs minimaux de A sont bornées supérieurement par une constante qui ne dépend que de f.

Considérons $\mathcal{E}$, l'ensemble des vecteurs $v \in \mathbb{Z}^n$ dont les composantes sont, en valeur absolue, inférieures à cette constante. Cet ensemble est bien évidemment fini. On peut définir une application qui, à chaque matrice A satisfaisant les hypothèses du lemme, fait correspondre une partie de $\mathcal{E}$: l'ensemble des vecteurs minimaux de A. Vu que les matrices A sont associées à des formes parfaites de minimum 1, cette application est injective, ce qui permet de conclure.

Pour démontrer la connexité du graphe de Voronoï, il suffit de montrer que deux domaines quelconques $\mathcal{C}$ et $\mathcal{C}'$ sont toujours connectés. Pour cela, considérons f, un point intérieur de $\mathcal{C}'$. f est toujours la matrice d'une forme quadratique définie positive.

Comme f est un point intérieur de $\mathcal{C}'$, si f appartient à $\mathcal{C}$, alors $\mathcal{C} = \mathcal{C}'$. Si, par contre, f n'appartient pas à $\mathcal{C}$, on peut trouver un hyperplan d'appui π de ce domaine, définissant une face de $\mathcal{C}$, tel que $\mathcal{C}$ et f se situent de part et d'autre de π. On recommence alors le raisonnement en remplaçant $\mathcal{C}$ par son domaine voisin relativement à la face $\pi \cap \mathcal{C}$.

Le lemme garantit que le processus s'arrête après un nombre fini d'itérations. En effet, $f \cdot A$, où A est la matrice de la forme parfaite de minimum 1 associé au domaine testé $(\mathcal{C})$, décroît strictement lors de chaque itération.

Considérons, maintenant, l'action de $Gl_n(\mathbb{Z}) \times \mathbb{R}^+$ sur l'ensemble $\mathcal{P}_n$ des formes parfaites à n variables :

$$\alpha : (Gl_n(\mathbb{Z}) \times \mathbb{R}^+) \times \mathcal{P}_n \to \mathcal{P}_n, \ (S;\lambda) \cdot q = \lambda q \circ S^{-1}.$$

Les orbites de cette action correspondent aux classes d'équivalence des formes parfaites.

THÉORÈME 9. — *L'action α décompose $\mathcal{P}_n$ en un nombre fini d'orbites.*

Pour la démonstration, on se référera, par exemple, à [Vo1] ou à [Oe1].

Considérons la représentation σ de $Gl_n(\mathbb{Z})$ sur l'espace de Voronoï $\mathcal{V}$:

$$\begin{array}{ccccccc} \sigma : & Gl_n(\mathbb{Z}) & \to & Gl(\mathcal{V}) & & & \\ & S & \mapsto & \sigma_s : & \mathcal{V} & \to & \mathcal{V} \\ & & & & X & \mapsto & SXS^t. \end{array}$$

Si $a_k = v_k v_k^t$ caractérise une arête du domaine associé à q, $\sigma_S(a_k)$ caractérise une arête du domaine associé à $q \circ S^{-1}$. Par linéarité, on conclut que σ_S transforme le domaine associé à q en le domaine associé à $q \circ S^{-1} = \alpha((S;1);q)$, et crée une bijection entre les faces de ces deux domaines.

Mieux : la permutation des domaines associés aux formes parfaites, induite par σ_S, est compatible avec la relation "être voisins". Par conséquent, σ permet de définir une action de $Gl_n(\mathbb{Z})$ sur le graphe de Voronoï.

On dira que deux domaines sont équivalents s'ils appartiennent à la même orbite. On montre facilement que deux domaines sont équivalents si et seulement si les formes parfaites correspondantes sont équivalentes. Il n'existe donc qu'un nombre fini de classes d'équivalence de domaines.

Le stabilisateur d'une forme parfaite par l'action α est un sous-groupe de $Gl_n(\mathbb{Z}) \times \{1\}$. Sa projection sur $Gl_n(\mathbb{Z})$ est appelée *groupe des automorphismes* de cette forme. Il faut donc comprendre "automorphisme" dans le sens d'isométries entières de cette forme.

Observons que le groupe des automorphismes d'une forme parfaite peut également être défini comme le stabilisateur du domaine associé à cette forme, par l'action de $Gl_n(\mathbb{Z})$ sur le graphe de Voronoï. En effet, soit q, une forme parfaite, et $\mathcal{C}$, le domaine qui lui est associé ; $S \in Gl_n(\mathbb{Z})$ est un automorphisme de q si et seulement si $q \circ S^{-1} = q$, c'est-à-dire $\sigma_S(\mathcal{C}) = \mathcal{C}$ puisque q est parfaite.

Pour rendre fidèle l'action du groupe des automorphismes d'une forme parfaite sur l'ensemble des arêtes du domaine associé à cette forme, il suffit de quotienter le groupe des automorphismes par $\pm$ identité, puisque toute forme parfaite est connectée au sens de Coxeter [Co1]. J'appellerai le groupe ainsi obtenu le *groupe des symétries* du domaine.

Finalement, il est clair que le groupe des automorphismes d'une forme parfaite est un groupe fini, puisque, si $\pm v_1, \pm v_2, ..., \pm v_s$ sont les vecteurs minimaux de cette forme, son groupe des automorphismes s'injecte de façon évidente dans le groupe des permutations de $2s$ éléments.

7. Un théorème de symétrie à propos des graphes localement finis.

Soit Γ, un graphe localement fini, $\mathcal{S}$, l'ensemble de ses sommets et $\mathcal{A}$, l'ensemble de ses arêtes. On définit deux applications naturelles :

$$\begin{array}{rccll} \mathfrak{A}: & \mathcal{S}\times\mathcal{S} & \to & \{0,1\} & \\ & (x;y) & \mapsto & \begin{cases} 1 \\ 0 \end{cases} & \begin{array}{l} \text{si } x \text{ et } y \text{ sont liés par une arête} \\ \text{sinon} \end{array} \end{array}$$

$$\begin{array}{rccll} \mathfrak{S}: & \mathcal{A} & \to & \mathcal{P}(\mathcal{S}) & \text{injective} \\ & a & \mapsto & \{x_a, y_a\} & \begin{array}{l} \text{où } x_a \text{ et } y_a \text{ sont les deux sommets} \\ \text{de } \Gamma \text{ liés par l'arête } a. \end{array} \end{array}$$

Soit un groupe G opérant sur Γ. G opère également sur $\mathcal{S}$ et $\mathcal{A}$, et il y a compatibilité de ces deux actions. Il existe donc deux actions, disons

$\alpha_{\mathcal{S}}$ et $\alpha_{\mathcal{A}}$,

$$\begin{array}{rccc} \alpha_{\mathcal{S}}: & G\times\mathcal{S} & \to & \mathcal{S} \\ & (g;x) & \mapsto & g\cdot x \end{array} \quad \text{et} \quad \begin{array}{rccc} \alpha_{\mathcal{A}}: & G\times\mathcal{A} & \to & \mathcal{A} \\ & (g;a) & \mapsto & g\cdot a \end{array}$$

satisfaisant les propriétés suivantes de compatibilité :

(i) $\mathfrak{A}(x,y) = \mathfrak{A}(g\cdot x, g\cdot y)$, $\forall g \in G$ et $\forall x, y \in \mathcal{S}$

(ii) $\mathfrak{S}(g\cdot a) = \{g\cdot x_a, g\cdot y_a\}$, $\forall g \in G$ et $\forall a \in \mathcal{A}$

ou encore $\{x_{g\cdot a}, y_{g\cdot a}\} = \{g\cdot x_a, g\cdot y_a\}$, $\forall g \in G$ et $\forall a \in \mathcal{A}$.

DÉFINITIONS. — *On dira que deux sommets x et y sont voisins si $\mathfrak{A}(x,y) = 1$. On appellera voisin de x, tout sommet y de Γ tel que $\mathfrak{A}(x,y) = 1$.*

Considérons, dans un premier temps, $\alpha_{\mathcal{S}}$, l'action de G sur l'ensemble $\mathcal{S}$ des sommets du graphe. Cette action partitionne $\mathcal{S}$ en orbites.

Soit $O_x = \{x_1, x_2, ..., x_i, ...\}$, une telle orbite, et x, un sommet quelconque de O_x. Appelons V_x, l'ensemble des sommets voisins de x et G_x, le stabilisateur de x dans G.

On peut considérer la restriction de $\alpha_{\mathcal{S}}$ à $G_x \times V_x$. Cette restriction nous fournit une action α_x de G_x sur V_x. Cette action partitionne V_x en orbites. On appellera ces orbites, les *orbites de voisins* de x ; le nombre d'orbites de voisins de x est fini puisque, par hypothèse, le graphe est localement fini. Notons V_x^j, la $j^{\text{ème}}$ orbite de voisins de x. Si deux sommets appartiennent à la même orbite V_x^j, il est clair qu'ils sont également dans la même orbite lorsqu'on regarde l'action de G sur $\mathcal{S}$.

Soit maintenant $O_x = \{x_1, x_2, ..., x_i, ...\}$ et $O_y = \{y_1, y_2, ..., y_i, ...\}$, deux orbites de sommets, distinctes ou non, par rapport à l'action de G sur $\mathcal{S}$. Pour x, un sommet quelconque de O_x, on définit la fonction suivante :

$$f(x, O_y) = \sum_i \chi(V_x^i, O_y) \text{ où } \chi(V_x^i, O_y) \text{ vaut 1 si } V_x^i \subset O_y, \text{ et 0 sinon.}$$

$f(x, O_y)$ compte le nombre d'orbites de voisins de x, contenues dans O_y.

THÉORÈME 10. — *Avec les notations ci-dessus :*

(i) *$f(x, O_y)$ est constante lorsque x parcourt O_x.*

On peut donc parler de $f(O_x, O_y)$.

(ii) *Avec la remarque du point (i), f est symétrique, c'est-à-dire* $f(O_x, O_y) = f(O_y, O_x)\ \forall O_x, O_y$.

Démonstration. — (i) Soit x et x', deux sommets de la même orbite O_x. On doit démontrer que $f(x, O_y) = f(x', O_y)\ \forall O_y$.

Comme x et x' sont dans la même orbite, il existe $g \in G$ tel que $g \cdot x = x'$.

Soit $V_x^1, V_x^2, ..., V_x^k, ..., V_x^q$, les orbites de voisins de x.

Les translatés par g des orbites de voisins de x donnent les orbites de voisins de x'. On peut donc numéroter les orbites de voisins de x' de telle manière que $V_{x'}^k = g \cdot V_x^k\ \forall k$.

En observant que V_x^k et $V_{x'}^k$ sont contenues dans la même orbite de $\mathcal{S}$ par rapport à l'action $\alpha_{\mathcal{S}}$, on déduit que $\chi(V_x^k, O_y) = \chi(V_{x'}^k, O_y)\ \forall k, \forall O_y$. En particulier, $f(x, O_y) = f(x', O_y)$ quelle que soit l'orbite O_y considérée.

(ii) Si $O_x = O_y$, il n'y a rien à démontrer. Supposons $O_x \neq O_y$.

Remarquons d'abord que la relation "être voisin de" est symétrique. Par conséquent, $f(O_x, O_y) = 0$ si et seulement si $f(O_y, O_x) = 0$. On supposera donc que $f(O_x, O_y) > 0$.

Soit y_1 et y_2, deux sommets voisins de x, distincts ou non, contenus dans O_y.

Il existe $g \in G$ tel que $y_2 = g \cdot y_1$. Choisissons un quelconque y dans O_y ; on trouvera $g_i \in G$ tels que $y = g_i \cdot y_i$ $(i = 1, 2)$.

Remarque : $1 = \mathfrak{A}(x, y_i) = \mathfrak{A}(g_i \cdot x, g_i \cdot y_i) = \mathfrak{A}(g_i \cdot x, y)$ signifie que $g_1 \cdot x$ et $g_2 \cdot x$ sont voisins de y.

Si $g_1 \cdot x$ et $g_2 \cdot x$ sont dans la même orbite de voisins de y, il existe $h' \in G_y$, tel que $h'(g_1 \cdot x) = g_2 \cdot x$. Dans ce cas, $h = (g_2^{-1} h' g_1)$ appartient à G_x, et envoie y_1 sur y_2.

Par conséquent, si y_1 et y_2 appartiennent à des orbites de voisins de x différentes, $g_1 \cdot x$ et $g_2 \cdot x$ doivent aussi appartenir à des orbites de voisins de y différentes.

Ainsi, $f(O_x, O_y) = f(x, O_y) \leq f(y, O_x) = f(O_y, O_x)$.

En échangeant les rôles de O_x et O_y, on obtient $f(O_y, O_x) \leq f(O_x, O_y)$, ce qui termine la démonstration.

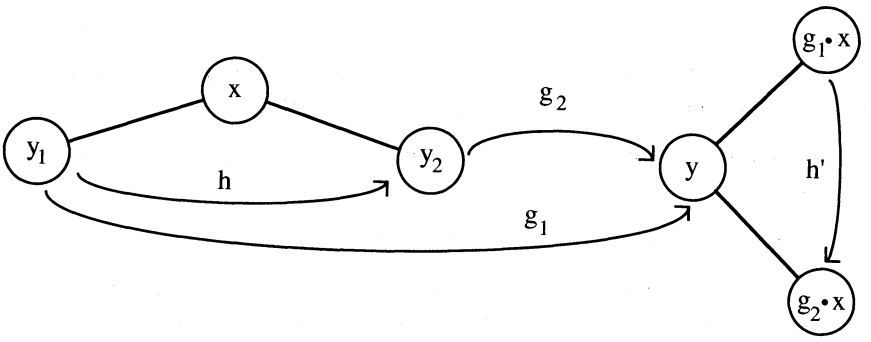


Figure 3

8. Algorithme de Voronoï.

8.1. Description.

Cet algorithme permet de calculer tous les maxima locaux de la fonction μ et, en particulier, la valeur de γ_n. On peut vérifier que, modulo les homothéties, tous les maxima locaux de μ sont isolés.

L'algorithme de Voronoï ramène le calcul des formes extrêmes à l'énumération complète des classes de formes parfaites. En effet, Voronoï commence par démontrer son fameux théorème : *une forme quadratique définie positive est extrême si et seulement si elle est parfaite et eutactique.*

On rencontre dans la littérature plusieurs démonstrations de ce théorème. A part celle de Voronoï lui-même, je citerai, entre autres, celle de Barnes [Ba4], basée sur un lemme de Stiemke [Sti1], celle de Martin Kneser utilisant la géométrie des convexes [Kn1] et celle, plus générale, d'Anne-Marie Bergé et de Jacques Martinet [BM2].

Pour obtenir une énumération complète, à équivalence près, des formes parfaites à n variables, l'algorithme de Voronoï se base, d'une part, sur la connexité du graphe de Voronoï, d'autre part, sur la finitude du nombre de classes d'équivalence des domaines associés aux formes parfaites.

Partant d'un domaine quelconque, on mémorisera sa classe d'équivalence et on déterminera tous ses domaines voisins. Certains d'entre eux n'appartiendront peut-être pas à la classe de départ. Dans ce cas, on obtiendra une liste de nouvelles classes d'équivalence. On mémorisera ces

nouvelles classes et, pour chacune d'entre elles, on choisira un représentant. Pour chacun de ces représentants, on déterminera à nouveau ses domaines voisins, domaines qui, à leur tour, caractériseront parfois de nouvelles classes, etc.

La connexité du graphe garantit qu'en réitérant ce processus toutes les classes seront atteintes, quel que soit le domaine de départ choisi. La finitude du nombre de classes d'équivalence prouve que l'algorithme s'arrête.

L'énumération de toutes les classes de domaines associés aux formes parfaites (donc de toutes les classes de formes parfaites) est complète lorsque, pour chaque classe connue, les voisins d'un représentant quelconque appartiennent tous à des classes déjà connues.

8.2. Symétries.

Dans la pratique, pour déterminer tous les domaines voisins d'un domaine, il faut d'abord calculer toutes les faces de ce domaine. C'est un problème de programmation linéaire entière dont la complexité croît très rapidement en fonction du nombre s de paires de vecteurs minimaux.

Soit q, une forme parfaite et D, le domaine qui lui est associé. Le groupe des symétries de D agit sur les faces de D. On dira que deux faces sont équivalentes si elles appartiennent à la même orbite. Il est clair que deux faces équivalentes donneront lieu à deux domaines voisins équivalents. Pour appliquer l'algorithme de Voronoï, il suffit de connaître au moins une face dans chaque orbite.

Géométriquement, cela revient à utiliser les symétries des domaines, ce qui simplifie parfois considérablement le problème. On trouvera une illustration de cette simplification dans [JS1].

8.3. Calcul des faces d'un domaine.

Lorsque le nombre d'arêtes d'un cône convexe C est égal à sa dimension d, le calcul des faces est instantané. Il suffit, en effet, de retirer à tour de rôle chacune des arêtes; celles qui restent déterminent une face.

Par contre, lorsque le nombre d'arêtes est supérieur à cette dimension, il faut remarquer que, si l'on aborde la recherche des faces d'un point de vue combinatoire (test de tous les $(d-1)$-tuples d'arêtes), le problème explose

rapidement. C'est là qu'interviennent mes algorithmes de la cascade et de l'explorateur.

8.3.1. Algorithme de la cascade.

Considérons le relèvement de $\mathcal{C}$ (cf. 4.2) avec $d = \dim C = N = \frac{n(n+1)}{2}$. On supposera que $\mathcal{C}$ possède s arêtes.

L'algorithme de la cascade se base sur le théorème fondamental du relèvement (th. 4, cf. 4.2.2) qui garantit que toute face de $\mathcal{C}^{k-1}$ peut s'obtenir par projection par π^k, soit d'une face de $\mathcal{C}^k$, soit de l'intersection de deux faces de $\mathcal{C}^k$.

Le principe de cet algorithme consiste à calculer d'abord les faces de $\mathcal{C}^s$ (sommet de la cascade), puis, à partir des faces de $\mathcal{C}^s$, à calculer celles de $\mathcal{C}^{s-1}$ (premier saut) en employant le fait que $\mathcal{C}^{s-1} = \pi^s(\mathcal{C}^s)$, puis, à partir des faces de $\mathcal{C}^{s-1}$, à calculer celles de $\mathcal{C}^{s-2}$ (second saut) en employant le fait que $\mathcal{C}^{s-2} = \pi^{s-1}(\mathcal{C}^{s-1})$, et ainsi de suite, jusqu'au dernier saut qui, à partir des faces de $\mathcal{C}^{N+1}$, permet de calculer celles de $\mathcal{C}^N$.

Dans ce qui suit, on considérera $\mathcal{C}$, un domaine de Voronoï associé à une forme parfaite q.

Un élément du groupe des symétries de ce domaine peut être représenté indifféremment et fidèlement par une matrice dans $Gl_n(\mathbb{Z})$, par un automorphisme de l'espace de Voronoï qui conserve le domaine, ou par une permutation des arêtes du domaine.

Par ce qui précède, le groupe des symétries de ce domaine peut être vu comme un groupe G d'automorphismes de E^N qui conserve $\mathcal{C}$. Le relèvement de $\mathcal{C}$ ordonne les arêtes du domaine. Pour $k = N, ..., s$, définissons G^k par :

$$G^k = \{g \in G \mid g \text{ fixe les } k - N, \text{ dernières arêtes du domaine}\}.$$

Il est clair que $G = G^N > G^{N+1} > ... > G^s$. D'autre part, il y a une représentation canonique de G^k sur $E^k \supset E^N$:

$$\begin{array}{ccc} G^k & \to & Gl(E^k) \\ g & \mapsto & g^k : E^k = E^N \oplus E^\perp \to E^k = E^N \oplus E^\perp \\ & \text{avec} & g^k \mid_{E^N} = g \text{ et } g^k \mid_{E^\perp} = \text{identité}. \end{array}$$

Comme $g \in G^k$ laisse fixes les $k - N$ dernières arêtes de $\mathcal{C}$, g^k laisse fixes les $k - N$ dernières arêtes de $\mathcal{C}^k$. Par construction, seules, exactement,

les $k - N$ dernières arêtes de $\mathcal{C}^k$ ne sont pas dans E^N. Ainsi, g^k est un automorphisme de E^k qui conserve $\mathcal{C}^k$. Cette remarque nous permet de définir le groupe des symétries de $\mathcal{C}^k$; il s'agit de l'image de G^k par la représentation ci-dessus.

Dans la pratique, calculer G^k peut être très long. On se contentera en général d'un sous-groupe. Soit donc $G = G^N = H^N > H^{N+1} > ... > H^s$ avec, pour tout k, $H^k < G^k$.

Dans ce qui suit, une telle suite de sous-groupes H^k sera fixée définitivement ; de plus, on représentera H^k comme un sous-groupe de permutations des arêtes du domaine, ce qui permet d'identifier canoniquement H^k et son image par la représentation ci-dessus.

Par un élément de H^k, toute facette de $\mathcal{C}^k$ est transformée en une facette de $\mathcal{C}^k$ de même dimension. On dira que deux facettes de $\mathcal{C}^k$ sont équivalentes s'il existe un élément de H^k qui envoie la première sur la seconde.

Plus généralement, si l'on considère l'ensemble des arêtes de $\mathcal{C}^k$, on peut définir une notion d'équivalence entre deux parties de cet ensemble. Deux parties sont équivalentes s'il existe un élément de H^k qui envoie la première sur la seconde. Comme $H^k < H^{k-1}$, on observe que ces équivalences sont compatibles avec la projection π^k qui envoie $\mathcal{C}^k$ sur $\mathcal{C}^{k-1}$.

On dira qu'une partie de l'ensemble des arêtes d'un cône convexe de dimension maximale caractérise une face F donnée de ce cône si les arêtes de cette partie sont dans F et si l'enveloppe linéaire des représentants des arêtes de cette partie est un sous-espace de codimension 1.

Ecrivons les orbites de faces de $\mathcal{C}^k$ sous l'action de H^k en mettant en évidence un représentant pour chaque orbite :

$(F_1^k, F_{1,2}^k, ..., F_{1,t_1}^k)$, représentant F_1^k ;

$(F_2^k, F_{2,2}^k, ..., F_{2,t_2}^k)$, représentant F_2^k ;

etc.

LEMME 8. — *Si une face de $\mathcal{C}^{k-1}$ est caractérisée par la projection des arêtes contenues dans l'intersection de deux faces de $\mathcal{C}^k$, elle est équivalente par l'action de H^{k-1} à une face caractérisée par la projection des arêtes contenues dans l'intersection de deux faces de $\mathcal{C}^k$, où la première face est le représentant choisi de son orbite.*

Démonstration. — Soit deux orbites de faces de $\mathcal{C}^k$, $\mathcal{O}$ et $\mathcal{O}'$ (distinctes ou non), $\mathcal{O} = \{F = F_1^k, F_2^k, ..., F_t^k\}$ et $\mathcal{O}' = \{F' = F'^k_1, F'^k_2, ..., F'^k_{t'}\}$. Soit encore $F_i^k \in \mathcal{O}$ et $F'^k_j \in \mathcal{O}'$, deux faces de $\mathcal{C}^k$.

Supposons que les arêtes de $\pi^k(F_i^k \cap F'^k_j)$ caractérisent une face de $\mathcal{C}^{k-1}$.

Comme F et F_i^k appartiennent à $\mathcal{O}$, il existe $g \in H^k$, tel que $F = g \cdot F_i^k$.

Comme g appartient à $H^k < H^{k-1}$, g doit appartenir à H^{k-1} ; ainsi, affirmer que les arêtes de $\pi^k(F_i^k \cap F'^k_j)$ caractérisent une face de $\mathcal{C}^{k-1}$ équivaut à dire que les arêtes de $g \cdot (\pi^k(F_i^k \cap F'^k_j))$ caractérisent une face de $\mathcal{C}^{k-1}$, face qui est équivalente à la première par l'action de H^{k-1}.

On vérifiera sans peine que π^k et g commutent, en observant que la permutation des indices des arêtes induite par π^k n'est autre que la permutation identité.

Ainsi, dire que les arêtes de $g \cdot (\pi^k(F_i^k \cap F'^k_j))$ caractérisent une face de $\mathcal{C}^{k-1}$, revient à dire que les arêtes de $\pi^k(g \cdot (F_i^k \cap F'^k_j))$ caractérisent une face de $\mathcal{C}^{k-1}$. On peut maintenant conclure en remarquant que :

$$g \cdot (F_i^k \cap F'^k_j) = (g \cdot F_i^k) \cap (g \cdot F'^k_j) = F \cap (g \cdot F'^k_j).$$

Ce lemme technique permet d'éviter un nombre parfois considérable de tests de faces potentielles, lorsqu'on effectue un saut dans l'algorithme de la cascade.

Pour fixer les idées, si $\mathcal{C}^k$ possède x orbites contenant chacune y faces, le rapport entre le nombre de cas testés en appliquant le lemme 8 et le nombre de cas testés sans employer ce lemme est donné par $\frac{x+1}{xy+1}$, qui est de l'ordre de $\frac{1}{y}$.

8.3.2. Algorithme de l'explorateur.

Lorsque la taille d'un domaine (différence entre son nombre d'arêtes et sa dimension) est grande (empiriquement supérieure à 8), l'algorithme de la cascade n'est plus assez efficace. En particulier, les domaines associés à E_6 et à E_7 y résistent. L'utilisation de l'algorithme de l'explorateur se révèle indispensable.

L'algorithme de l'explorateur est avant tout basé sur la notion de faces voisines, notion développée dans le paragraphe 4.3. Cet algorithme se

base sur les corollaires du théorème 7 en utilisant, de plus, le groupe des symétries du domaine, ce qui localise considérablement le problème et, par conséquent, le simplifie.

D'une certaine manière, l'algorithme de l'explorateur est un algorithme de Voronoï pour les faces d'un domaine, un algorithme de Voronoï en profondeur.

La première phase consiste à récolter les faces du domaine déjà connues. Pratiquement, dans les cas qui nous intéressent, on trouve toujours parmi ces faces au moins une face qui n'est pas maximale. Si tel n'était pas le cas, il faudrait en calculer une; mais il est toujours facile de trouver une face, même non maximale; la difficulté est de s'assurer qu'on les a toutes à équivalence près! L'existence de faces non maximales est garantie par le corollaire 1 du théorème 7.

Parmi les faces récoltées, on en retiendra une par classe d'équivalence rencontrée, c'est-à-dire par orbite sous l'action du groupe des symétries du domaine. Pour chaque face retenue non maximale, on calculera l'ensemble de ses faces voisines. Parmi toutes ces faces voisines, certaines, probablement, seront équivalentes à une face déjà rencontrée; d'autres, peut-être, seront nouvelles. On continuera l'exploration à partir de ces nouvelles faces.

Plus précisément, pour chaque nouvelle orbite rencontrée de faces non maximales, on choisira un représentant pour lequel on calculera toutes les faces voisines et ainsi de suite, jusqu'à ce que toutes les faces voisines de toutes les faces non maximales connues soient équivalentes à une des faces connues.

La connexité du graphe des faces d'un domaine garantit alors qu'on a un représentant de chaque orbite. Le procédé s'arrête puisque le nombre de faces étant fini, le nombre d'orbites, a fortiori, est aussi fini.

Il faut tout de même faire la remarque évidente suivante : si deux faces sont équivalentes, toute face voisine de la première est équivalente à une face voisine de la seconde.

Le problème est maintenant le suivant : étant donné une face F d'un domaine, calculer ses faces voisines.

L'intersection de F avec une de ses faces voisines est une facette de codimension 2 du domaine donc, par le lemme 2, une face de F.

Inversement, si f est une face de F, par le lemme 1, f est une facette de codimension 2 du domaine. Par le lemme 5, seules exactement deux

faces du domaine contiennent f. La face F en est une ; l'autre est une face voisine de F ; c'est la face voisine de F, par rapport à f.

Par conséquent, il s'agit de calculer les faces de F.

Considérons H, le sous-groupe des symétries du domaine qui stabilise la face F.

H agit sur les faces de F et les organise en orbites. On dira que deux faces f_1 et f_2 de F sont équivalentes si elles appartiennent à la même orbite.

Il est facile de voir qu'à deux faces équivalentes de F correspondent deux faces voisines équivalentes ; cette remarque nous permet de prendre H comme groupe des symétries de F.

Pour appliquer l'algorithme de l'explorateur, il suffit de calculer les faces de F, à équivalence près.

8.3.3. Fusion de ces deux algorithmes.

L'algorithme de l'explorateur ramène, d'une certaine manière, le calcul des faces d'un domaine au calcul des faces de ses faces. Une face F d'un domaine D est aussi un cône convexe saillant. On désire calculer les faces de ce cône convexe F modulo l'action d'un groupe H de symétries.

Si la taille de F est petite, on appliquera comme précédemment l'algorithme de la cascade mais, cette fois-ci, au cône convexe saillant F. Si, par contre, la taille de F est trop grande, on fera appel récursivement à l'algorithme de l'explorateur pour calculer les faces de F.

L'algorithme de l'explorateur appliqué à F ramène le calcul des faces de F au calcul des faces des faces de F et ainsi de suite : si f est une face de F, le calcul des faces de f sera effectué par l'algorithme de la cascade si la taille de f est petite, ou par l'algorithme de l'explorateur appliqué récursivement à f, si la taille de f est encore trop grande.

L'algorithme de l'explorateur contourne les faces maximales. Ainsi, un appel à cet algorithme diminue toujours, non seulement la dimension, mais également la taille des cônes convexes saillants sur lesquels on espère pouvoir appliquer l'algorithme de la cascade, ce qui garantit l'efficacité de l'exploration.

L'utilisation récursive de l'algorithme de l'explorateur crée des chaînes de cônes convexes saillants, où chaque chaînon est une face du chaînon précédent :

$\mathcal{C} = \mathcal{C}_0 \supset \mathcal{C}_1 \supset \mathcal{C}_2 \supset \ldots \supset \mathcal{C}_t$, où pour $i \geq 1$, $\mathcal{C}_i$ est un cône convexe saillant, face de $\mathcal{C}_{i-1}$ et facette de codimension i de $\mathcal{C}$.

Nous appellerons une telle chaîne une *chaîne inclusive de faces.*

Si $G = H_0$ est le groupe des symétries de $\mathcal{C}$, on définit inductivement, pour i compris entre 1 et t, H_i, le groupe des symétries de $\mathcal{C}_i$ par la condition suivante : H_i est le sous-groupe de H_{i-1} qui stabilise $\mathcal{C}_i$. Cette définition des H_i garantit qu'à deux faces de $\mathcal{C}_i$, équivalentes par l'action de H_i, correspondent deux faces de $\mathcal{C}_{i-1}$, voisines de $\mathcal{C}_i$, équivalentes par l'action de H_{i-1}.

8.5. Identification automatique des voisines.

Géométriquement, en terme de réseaux, il s'agit, en fait, de résoudre automatiquement (et si possible rapidement !) le problème suivant :

Soit deux réseaux de $\mathbb{R}^n$ donnés par les matrices de Gram de deux de leurs bases respectives ; ces deux réseaux sont-ils équivalents ?

Dans ce qui suit, on utilisera plutôt le langage des formes quadratiques.

Soit deux formes quadratiques définies positives données par les matrices A et B qui leur sont associées. Ces deux formes sont équivalentes si et seulement si il existe un nombre réel positif λ et une matrice S dans $GL_n(\mathbb{Z})$, tels que $A = \lambda S^t B S$.

Après normalisation éventuelle, on peut supposer A et B de même minimum et de même déterminant. Notre problème consiste à exhiber, si elle existe, une matrice S à coefficients entiers, telle que $A = S^t B S$.

Considérons $v_1, v_2, \ldots, v_p$ ($v_i \in \mathbb{Z}^n$), un quelconque système de générateurs de $\mathbb{Z}^n$. Nous allons voir que S existe si et seulement si on peut trouver $w_1, w_2, \ldots, w_p (w_i \in \mathbb{Z}^n)$ tels que $v_i^t A v_j = w_i^t B w_j$ $(\forall i, j)$.

Si S existe, il suffit de poser $w_i = S v_i$, $i = 1, 2, \ldots, p$.

Pour montrer la réciproque, considérons V (resp. W), la matrice dont les colonnes sont les v_i (resp. les w_i).

L'hypothèse devient $V^t A V = W^t B W$.

Dire que les v_i forment un système de générateurs de $\mathbb{Z}^n$ revient à dire qu'il existe une matrice U à p lignes et n colonnes, à coefficients entiers, telle que le produit $V\,U$ soit égal à la matrice identité.

Posons $S = WU$. La matrice S est à coefficients entiers et vérifie $A = S^t BS$.

D'un point de vue algorithmique, étant donné $v_1, v_2, ..., v_p$, un système bien choisi de générateurs de $\mathbb{Z}^n$, la recherche des $w_1, w_2, ..., w_p$ sera une recherche en arbre avec une très forte heuristique, avant tout basée sur la notion de spectre.

Une variante de cet algorithme d'identification permet, par exemple, l'énumération de tous les automorphismes d'une forme parfaite. D'autres variantes automatisent le calcul du stabilisateur d'une face d'un domaine de Voronoï ou testent l'équivalence éventuelle entre facettes d'un même domaine.

9. Conclusion.

Les calculs que j'ai effectués sur ordinateur démontrent qu'il n'y a que trente-trois classes de formes parfaites en dimension sept, mais les résultats de ces calculs contiennent des informations beaucoup plus précises.

Ils permettent, par exemple, de connaître le nombre exact d'orbites de voisines d'une certaine forme parfaite, qui sont contenues dans une classe donnée; ils décrivent ainsi complètement l'évaluation de la fonction f du théorème 10 sur les classes d'équivalence des domaines de Voronoï.

Le tableau suivant résume cette information pour la dimension 7. Par le théorème 10, on sait qu'il doit être symétrique.

Finalement, cette classification démontre également le théorème suivant qui confirme et généralise plusieurs théorèmes dus à Watson :

THÉORÈME. — *Tout réseau parfait de dimension inférieure ou égale à sept possède une base formée de vecteurs minimaux.*

La description détaillée que j'ai obtenue des domaines de Voronoï en dimension inférieure ou égale à sept, peut être consultée à l'Université de Neuchâtel. De plus, un exemplaire complet et entièrement commenté des programmes LISP qu'il m'a fallu développer pour obtenir ces résultats est également disponible et déposé au même endroit. Le fascicule qui regroupe ces programmes comprend plus de 460 pages.

det. (min = 2)	s		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
2	63	1	11	1	6	4	10	6	18	10	1	8	9	1	3	7	1	3	6	4	1	2	2	7	2	5	5	3	3	5	6	2	4	1	
8192 / 2187	28	2	1																																
243 / 64	36	3	6		3	1		3	3	2	1								1					1				1			1				
4	42	4	4		1	1				1	1			1							1			1				1	1		1		1	1	1
4	36	5	10				6	1	7	2		2	4		1	3		1	1	2	1	1	1		1	2									
1024 / 243	32	6	6		3		1	2	2	1	1					1		1	1																
135 / 32	34	7	18		3		7	2	23	2		4	5			5	1	2	2	1		1	1	3	2	3	3		1	4			1		
9 / 2	32	8	10		2	1	2	1	2	1	1	1							1		1			1		1				1	1			
71344 / 15625	28	9	1		1	1		1		1				1																					
147 / 32	32	10	8				2		4	1		2	2							1					1	1				1		1			
1120 / 243	30	11	9				4		5			2	4		1	1	1		1	1					1	1									
10240 / 2187	28	12	1			1					1																								
4805 / 1024	28	13	3				1						1						1																
10336 / 2187	29	14	7				3	1	5				1			1	1	1		1			1	1			1								
38809 / 8192	28	15	1						1				1			1																			
128 / 27	30	16	3				1	1	2							1				1				1			1		1						
10528 / 2187	28	17	6		1		1	1	2	1			1		1																				
2465 / 512	28	18	4				2		1			1	1			1		1								1	1								
392 / 81	28	19	1			1	1			1																									
10658 / 2187	28	20	2				1		1																										
3584 / 729	28	21	2				1		1							1																	1		
315 / 64	30	22	7		1	1			3	1						1		1						1			1		1		1		1		
10780 / 2187	28	23	2				1		2			1	1																						
10808 / 2187	28	24	5				2		3	1		1	1							1										1		1			
11008 / 2187	28	25	5						3							1		1		1				1					1	1					
81 / 16	30	26	3		1	1																								1					
81 / 16	30	27	3			1			1									1						1			1			1			1		
81 / 16	30	28	5						4	1		1														1	1		1	1	1				
171 / 32	29	29	6		1	1				1														1				1		1			1	1	
343 / 64	28	30	2									1														1									
45 / 8	28	31	4			1			1														1	1						1		1		
189 / 32	28	32	1			1																							1		1				
8	28	33				1																													

Figure 4

Finalement, j'aimerais signaler que la tendance actuelle vise à une généralisation de l'algorithme de Voronoï, ou plutôt de son domaine d'application.

L'algorithme de l'explorateur s'intègre bien dans ce contexte, puisqu'il donne une généralisation, aussi bien du domaine d'application de l'algorithme de Voronoï (facettes d'un domaine), que de l'algorithme lui-même, en lui permettant d'agir récursivement, en profondeur.

BIBLIOGRAPHIE

[Ba1] E.S. BARNES, Note on extreme forms, Can. J. Math., 7 (1955), 150-154.

[Ba2] E.S. BARNES, The perfect and extreme senary forms, Can. J. Math., 9 (1957), 235-242.

[Ba3] E.S. BARNES, The complete enumeration of extreme senary forms, Phil. Trans. R. Soc. Lond., A, 249 (1957), 461-506.

[Ba4] E.S. BARNES, On a theorem of Voronoï, Proc. Camb. Phil. Soc., 53 (1957), 537-539.

[Ba5] E.S. BARNES, Criteria for extreme forms, J. Aust. Math. Soc., 1 (1959), 17-20.

[BM1] A.-M. BERGÉ & J. MARTINET, Sur la constante d'Hermite (étude historique), Sém. de Th. des Nombres de Bordeaux 2, Exposé 8, pp. 8-01-8-15 (1985-1986).

[BM2] A.-M. BERGÉ & J. MARTINET, Sur un problème de dualité lié aux sphères en géométrie des nombres, J. of Number Theory, Vol. 32, No. 1 (1989), 14-42.

[Be1] M. BERGER, Géométrie 3 / convexes et polytopes, polyèdres réguliers, aires et volumes. Cedic, Fernand Nathan (publié avec le concours du C.N.R.S.) (1978).

[Bl1] H.F. BLICHFELDT, On the minimum value of positive real quadratic forms in 6 variables, Bull. Am. Math. Soc., 31, 386 (1925).

[Bl2] H.F. BLICHFELDT, The minimum value of quadratic forms, and the closest packing of spheres, Math. Annalen, 101 (1929), 605-608.

[Bl3] H.F. BLICHFELDT, The minimum values of quadratic forms in six, seven and eight variables, Math. Z., 39 (1935), 1-15.

[CS1] J.H. CONWAY & N.J.A. SLOANE, Sphere-packings, lattices and groups. Grundlehren der mathematischen Wissenschaften 290, Springer-Verlag, 1988.

[CS2] J.H. CONWAY & N.J.A. SLOANE, Low-dimensional lattices. III. Perfect forms, Proc. R. Soc. Lond., A, 418 (1988), 43-80.

[Co1] H.S.M. COXETER, Extreme forms, Can. J. Math., 3 (1851), 391-441.

[GS1] L. GUY & J.R. STEELE, Common LISP : The Language. Digital Press, 1984, 465 pages.

[JS1] D.-O. JAQUET & F. SIGRIST, Formes quadratiques contiguës à D7, C. R. Acad. Sci. Paris, t. 309, Série I (1989), 641-644.

[Ja1] D.-O. JAQUET, Domaines de Voronoï et algorithme de réduction des formes quadratiques définies positives. Sém. de Th. des Nombres de Bordeaux 2 (1990), 163-215.

[Ja2] D.-O. JAQUET, Classification des réseaux dans $\mathbb{R}_7$ (via la notion de formes parfaites), Astérisque, Soc. Math. de France, 198-199-200 (1991), 177-185.

[Kn1] M. KNESER, Two remarks on extreme forms, Can. J. Math., 7 (1955), 145-149.

[KZ1] A. KORKINE & G. ZOLOTAREFF, Sur les formes quadratiques, Math. Annalen, 6 (1873), 336-389.

[KZ2] A. KORKINE & G. ZOLOTAREFF, Sur les formes quadratiques positives, Math. Annalen, 11 (1877), 242-292.

[La1] J. LARMOUTH, The enumeration of perfect forms. Dans "Computers in number theory" (A. O. L. Atkin & B. J. Birch editors), pp. 237-239, New York, Academic Press 1971.

[Mo1] L.J. MORDELL, Observation on the minimum of a positive quadratic form in eight variables, J. Lond. Math. Soc., 19 (1944), 3-6.

[Oe1] J. OESTERLÉ, Empilements de sphères. Sém. N. Bourbaki 42, Exposé 727, Vol. 1989-90 (1990).

[Sc1] P.R. SCOTT, On perfect and extreme forms. Thesis, Department of Mathematics, Univ. of Adelaide (1963).

[Sc2] P.R. SCOTT, On perfect and extreme forms, J. Aust. Math. Soc., 4 (1964), 56-77.

[Sc3] P.R. SCOTT, The construction of perfect and extreme forms, Can. J. Math., Vol. 18 (1966), 147-158.

[Se1] J.-P. SERRE, Cours d'arithmétique. 2e édition, Presses Univ. de France, Paris, 1977.

[Si1] F. SIGRIST, Formes quadratiques encapsulées. Sém. de Th. des Nombres de Bordeaux, 2 (1990), 425-429.

[Su1] S.Sh. SUSHBAEV, Voronoï neighborhood of perfect form ϕ_{15} $(x_1, x_2, ..., x_7)$, Vop. Vychisl. Prikl. Mat., 77 (1985), 48-56.

[St1] K.C. STACEY, The enumeration of perfect quadratic forms in seven variables, Ph. D. Dissertation, University of Oxford, 1973.

[St2] K.C. STACEY, The enumeration of perfect septenary forms, J. Lond. Math. Soc. (2) 10 (1975), 97-104.

[St3] K.C. STACEY, The perfect septenary forms with $\Delta_4 = 2$, J. Aust. Math. Soc., (A) 22 (1976), 144-164.

[Sti1] E. STIEMKE, Über positive Lösungen homogener linearer Gleichungen, Math. Annalen, 76 (1915), 340-342.

[Ve1] N.M. VETCHINKIN, Uniqueness of the classes of positive quadratic forms on which the values of Hermite constants are attained for $6 \leq n \leq 8$, Trudy Mat. Inst. Imeni V. A. Steklova, 152 (1980), 34-86.
(traduction anglaise dans Proc. Steklov Inst. Math. (3) (1982), 37-95.

[Vo1] G. VORONOÏ, Sur quelques propriétés des formes quadratiques positives parfaites, J. reine angew. Math., 133 (1908), 97-178.

[Wa1] G.L. WATSON, On the minimum of a positive quadratic form in $n(\leq 8)$ variables (verification of Blichfeldt's calculation), Proc. Camb. Phil. Soc., 62 (1966), 719.

[Wa2] G.L. WATSON, On the minimal points of perfect septenary forms, Mathematika, 16 (1969), 170-177.

[Wa3] G.L. WATSON, Integral quadratic forms, Cambridge, University Press, 1970.

[Wa4] G.L. WATSON, On the minimal points of a positive quadratic form, Mathematika, 18 (1971), 60-70.

[Wa5] G.L. WATSON, The number of minimum points of a positive quadratic form, Dissertationes Math., 84 (1971), 1-46.

[Wa6] G.L. WATSON, The number of minimum points of a positive quadratic form having no perfect binary section with the same minimum, Proc. Lond. Math. Soc. (3) 24 (1972), 625-646.

Manuscrit reçu le 13 janvier 1992.

David-Olivier JAQUET-CHIFFELLE,
Institut de Mathématiques
Chantemerle 20
2007 Neuchâtel (Suisse).