N^0 d'ordre : 869

T H È S E

présentée à

L'UNIVERSITÉ BORDEAUX I

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : ALGORITHMIQUE ARITHMÉTIQUE

par

Mohamed LAÏHEM

CONSTRUCTION ALGORITHMIQUE DE RÉSEAUX PARFAITS

Soutenue le 04 Décembre 1992, devant la Commission d'Examen :

M	M. OLIVIER	Université Bordeaux I	*Président*
M	C. BATUT	Université Bordeaux I	
Mme	E. BAYER-FLUCKIGER	Université de Besançon	
Mme	A-M BERGÉ	Université Bordeaux I	*Examinateurs*
M	J. MARTINET	Université Bordeaux I	
M	F. SIGRIST	Université de Neuchâtel	

- 1992 -

TABLE DES MATIÈRES

INTRODUCTION

L'une des motivations de cette étude était de produire une table étendue de réseaux parfaits en dimension 8. Pour cela, on a mis au point un algorithme capable de trouver les réseaux parfaits à section hyperplane parfaite.

Pourquoi les réseaux *parfaits?*
En géométrie des nombres, la constante d'Hermite entre en jeu dans de nombreuses inégalités (comme par exemple les minorations de régulateurs). Cette constante correspond aux empilements réguliers de sphères les plus denses. Korkine et Zolotareff (1873) introduisent la notion de réseau extrême, c'est-à-dire réalisant un maximum local de la densité ; ils montrent en outre qu'un tel réseau est parfait (pour la définition voir 0.6). En 1908 Voronoï démontre que les réseaux parfaits sont en nombre fini à similitude près pour une dimension donnée. D'où l'intérêt de chercher les réseaux parfaits.

Parmi les réseaux parfaits pourquoi avoir choisi ceux à *section hyperplane parfaite ?*
On voudrait utiliser comme moyen de rechercher un algorithme décrit par Voronoï, et qui permet de trouver par contiguïté tous les réseaux parfaits en dimension n donnée. Cette méthode a été appliquée avec succès pour $n \leq 7$, les travaux s'échelonnant de 1908 à 1990 (date à laquelle on obtient la liste définitive des 48 réseaux parfaits).
Malheureusement dès que n dépasse 7, les calculs augmentent si rapidement de taille et de volume qu'ils deviennent prohibitifs pour les ordinateurs actuels. Avant ce travail on ne connaissait qu'une vingtaine de réseaux parfaits en dimension 8 (c.f 0.6).
Une variante de l'algorithme est alors d'imposer à ces réseaux parfaits une section hyperplane parfaite. Cela présente l'avantage de simplifier énormément la méthode ce qui se traduit par une économie considérable en temps d'éxécution.
Mis en oeuvre en dimension 8, ce procédé s'est avéré fécond puisqu'il a fourni un millier de réseaux parfaits en un temps raisonnable (étendant ainsi de façon considérable la liste des réseaux parfaits en dimension 8 connue à ce jour!) Il convient de signaler à ce propos que Jaquet vient d'obtenir l'énumération des 48 réseaux contigus du réseau de racines $\mathbb{D}_8$.

Cette thèse est composée de quatre chapitres :

Le premier rappelle d'abord quelques notions bien connues sur les réseaux, puis passe directement au problème des réseaux à section donnée. L'étude de la densité de ces réseaux conduit notamment à introduire une notion de perfection qui coïncide avec la notion classique lorsque la section elle-même est parfaite.

Le deuxième consiste essentiellement en une adaptation de l'algorithme de Voronoï à

notre situation propre. Si habituellement les calculs se font dans un espace euclidien de dimension $\frac{n(n+1)}{2}$, on verra pourquoi la dimension tombe à n si l'on impose au réseau parfait d'avoir une section hyperplane parfaite. On montre que cet algorithme fournit au bout d'un temps fini tous les réseaux cherchés.

Le troisième chapitre est purement algorithmique. C'est la partie la plus vécue de ce travail. Les notions qui étaient jusque là abstraites "bougent" et "s'affichent" à l'écran. Sont décrits tous les programmes qui ont permis l'établissement de la table, particulièrement les algorithmes de contiguïté, d'isométrie au sens restreint, et de tri.

Le quatrième chapitre exploite le catalogue des réseaux obtenus en dimension 8 à partir des 30 réseaux parfaits en dimension 7 autre que les 3 réseaux de racines. Nous faisons un inventaire des réseaux trouvés (résultat explosif : il y en a 1171!). La richesse de la table nous permet de répondre à certaines questions jusque là en suspens. La thèse s'achève par une analyse des nouveaux réseaux ("radiographies" , étude duale, ...).

Il restera à traiter le cas des 3 réseaux de racines, $\mathbb{E}_7$, $\mathbb{D}_7$, et $\mathbb{A}_7$. Pour trouver les contigus de $\mathbb{E}_7$, le temps d'exécution du programme de Jaquet a dépassé les 100 jours CPU sur un "VAX 8530". Dans notre cas, la présence du célèbre reseau $\mathbb{E}_8$, exigera la mise au point d'un programme plus performant.

N.B._ Les chapitres sont divisés en paragraphes. Les paragraphes ont une numérotation qui se suit à travers toute la thèse. Cela permet des renvois plus précis et plus brefs (exemple : c.f. 2.3 , voir le §2 au numéro 3).

Chapitre I

POSITION DU PROBLÈME

0. Rappels

Rappelons brièvement quelques définitions, propriétés et notations concernant les réseaux parfaits euclidiens.

On se donne un espace euclidien E de dimension n. Le produit scalaire de x et y dans E est noté x.y . Le nombre réel $\|x\| = \sqrt{x.x}$ représente la distance euclidienne de x à l'origine 0 de E; à ne pas confondre avec la *norme* N(x) = x.x qui est le carré de cette distance.

0.1 Réseaux, norme, vecteurs minimaux, discriminant, déterminant.

Un *réseau* Λ de E est un $\mathbb{Z}$-module libre engendré par une base $\mathfrak{B} = \{ e_1, e_2, ..., e_n \}$ de E; il est donc de rang n. $\mathfrak{B}$ est encore appelée *base* du réseau.

La *norme* de Λ est le nombre

$$N(\Lambda) = \inf_{\substack{x \in \Lambda \\ x \neq 0}} N(x),$$

(et par analogie on pose $\|\Lambda\| = \sqrt{N(\Lambda)}$).

Tout vecteur x de Λ tel que $N(x) = N(\Lambda)$ est appelé *vecteur minimal*. Il est clair que si x est minimal, -x l'est aussi. L'ensemble des vecteurs minimaux de Λ,

$$S(\Lambda) = \{ x \in \Lambda \mid N(x) = N(\Lambda) \}$$

(appelé aussi *sphère* de Λ), a donc un cardinal pair. On note $s(\Lambda) = \frac{1}{2}|S(\Lambda)|$,où $|S(\Lambda)|$ représente le cardinal de l'ensemble $S(\Lambda)$.

Si $\mathcal{E} = \{ \varepsilon_1, \varepsilon_2, ..., \varepsilon_n \}$ est une base orthonormée de E, le *discriminant* du réseau Λ est le réel positif

$$\Delta(\Lambda) = \Delta(e_1, e_2, ..., e_n) = |\det_{\mathcal{E}}(e_1, e_2, ..., e_n)| \ .$$

On montre facilement que $\Delta(\Lambda)$ est indépendant de la base orthonormée choisie; il représente le volume du *parallélotope* $P = \{ \sum_{i=1}^{n} \alpha_i e_i \mid 0 \leq \alpha_i < 1 \}$ construit sur la base $\mathfrak{B}$.

On appelle *déterminant* de Λ, le carré du discriminant, i.e : $\det(\Lambda) = \Delta(\Lambda)^2$.

Les inégalités suivantes relient ce déterminant et les normes des vecteurs de base :

* Inégalité de Hadamard : Si $e_1, e_2, ..., e_n$ sont n vecteurs indépendants d'un réseau Λ de E, alors

$$\det(\Lambda) \leq N(e_1).N(e_2)...N(e_n).$$

* Inégalité d'Hermite : Tout réseau Λ de E possède une base $\{ e_1, e_2, ..., e_n \}$ vérifiant

$$N(e_1).N(e_2)...N(e_n) \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} . \det(\Lambda).$$

On en déduit que le rapport $\gamma(\Lambda) = \dfrac{N(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}}$ appelé *fonction d'Hermite* (Hermite 1850), est majoré par $\left(\frac{4}{3}\right)^{\frac{n-1}{2}}$. C'est le maximum γ_n de cette fonction (appelé *constante d'Hermite*) qui a conduit Korkine et Zolotareff (c.f. [1]) à la notion de réseau parfait dont on parlera plus loin.

0.2 Matrice de Gram d'un réseau.

La *matrice de Gram* de Λ suivant la base $\mathfrak{B}$, est la matrice des produits scalaires $e_i.e_j$ notée $Gram(\Lambda, \mathfrak{B})$.

Elle est évidemment symétrique, et son déterminant est égal à $\det(\Lambda)$.

0.3 Lexique réseaux-formes quadratiques-matrices symétriques.

Nous donnons maintenant la correspondance réseaux - formes quadratiques - matrices symétriques :

Soit $(\Lambda, \mathfrak{B})$ un réseau de E rapporté à la base $\mathfrak{B}$. On note $A = (a_{ij})$ la matrice $Gram(\Lambda, \mathfrak{B})$ et q la forme quadratique sur $\mathbb{R}^n$ de matrice A. Cette forme est définie positive, et par abus de langage la matrice A est dite *définie positive.*

Si x est un élément de E et

$$\xi = \begin{pmatrix} \xi_1 \\ \vdots \\ \vdots \\ \xi_n \end{pmatrix}$$

la matrice de ses composantes dans la base $\mathfrak{B}$, alors on a

$$q(\xi) = N(x) = {}^t\xi A\xi = \sum a_{ij}\xi_i\xi_j.$$

Le déterminant de A n'est autre que le *discriminant* de la forme quadratique.

On a

$$N(\Lambda) = \min_{\xi \in \mathbb{Z}^n - \{0\}} q(\xi),$$

et les représentations $\xi_{(1)}, \xi_{(2)}, ..., \xi_{(s)}$ dans $\mathbb{R}^n$ des vecteurs minimaux (2 à 2 non opposés) $x_1, x_2, ..., x_s$ de Λ dans la base $\mathfrak{B}$ sont les *vecteurs minimaux de q* (et par abus de langage, *de la matrice A*).

De même, $N(\Lambda)$ est appelée *minimum* de q (ou de A).

0.4 Changement de base et équivalence.

* Soit $\mathfrak{B}'$ une autre base de Λ et $P \in Gl_n(\mathbb{Z})$ la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$. (On rappelle que $Gl_n(\mathbb{Z})$ est le groupe des matrices entières d'ordre n de déterminant ± 1).

Si

$$\xi' = \begin{pmatrix} {\xi'}_1 \\ {\xi'}_2 \\ \vdots \\ {\xi'}_n \end{pmatrix} \in \mathbb{Z}^n$$

représente un élément x de Λ dans $\mathfrak{B}'$, et

$$\xi = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} \in \mathbb{Z}^n$$

représente le même élément x dans $\mathfrak{B}$, alors on a :

$$\xi = P\xi'$$

D'où

$$Gram(\Lambda, \mathfrak{B}') = {}^tPAP$$

${}^tP$ étant la transposée de P. Donc à *un réseau* Λ *correspond une classe d'équivalence sous* $Gl_n(\mathbb{Z})$ *de matrices.*

* *Si* Λ' *est un réseau isométrique à* Λ, *ie* $\Lambda' = u\Lambda$ *pour* $u \in O(E)$ *(groupe orthogonal de E), alors*

$$Gram(\Lambda', u\mathfrak{B}) = (u(e_i).u(e_j)) = (e_i.e_j) = Gram(\Lambda, \mathfrak{B}).$$

D'où à une classe d'isométrie de réseaux est associée une classe d'équivalence (par $Gl_n(\mathbb{Z})$*) de matrices symétriques, et ceci définit une bijection.*

0.5 Endomorphismes symétriques.

On utilisera les notations classiques des objets mathématiques courants tels que :

* End(E) : ensemble des *endomorphismes* de E.

* Tr(u) : *trace* de l'endomorphisme u de End(E).

On sait que Tr(uv) = Tr(vu) $\forall\ u, v \in End(E)$.

* ${}^tu$: *transposé* de u.

Il est défini par

$${}^tu(x).y = x.u(y)\ \forall\ x, y \in E.$$

On rappelle que ${}^t(uv) = {}^tv{}^tu$, et ${}^t(u+v) = {}^tu + {}^tv$.

* $End^s(E)$: l'espace des endomorphismes *symétriques* de E, i.e. :

$$End^s(E) = \{\ u \in End(E) \mid {}^tu = u\ \}.$$

Il est bon de remarquer que si $u \in End(E)$, alors ${}^tuu$ *et* $({}^tuu - Id)$, sont dans $End^s(E)$; en particulier si $u \in End^s(E), u^2$ aussi.

Tout $u \in End^s(E)$ a ses valeurs propres λ_i réelles et il est toujours diagonalisable dans une base orthonormée de E. Si les λ_i sont $\geqslant 0$, on dit que u est *positif* (comme ${}^tuu$ par exemple); si les les λ_i sont > 0, on dit qu'il est *défini positif*, et dans ce cas il existe un unique $\sqrt{u} \in End^s(E)$ à valeurs propres > 0, tel que $(\sqrt{u})^2 = u$, et les valeurs propres de $\sqrt{u}$ sont les $\sqrt{\lambda_i}$.

0.6 Réseaux parfaits.

Nous allons définir maintenant la notion de *réseau parfait* introduite par Korkine et Zolotareff (c.f. [1]).

Soit $x \in E$; on désignera par φ_x la forme linéaire $u \to u(x).x$ sur $End^s(E)$. On dit qu'un réseau Λ de E est *parfait*, s'il vérifie l'une des propriétés suivantes qui sont équivalentes :

i)$\varphi_x(u) = 0\ \forall x \in S(\Lambda) \Rightarrow u = 0$.

ii)La matrice de Gram $A = Gram(\Lambda, \mathfrak{B})$ est déterminée de façon unique par la donnée de son minimum $N(\Lambda)$ et des composantes $\xi_{(1)}, \xi_{(2)}, ..., \xi_{(s)}$ dans $\mathfrak{B}$ des vecteurs minimaux de Λ non 2 à 2 opposés, via le système

$$^t\xi_{(i)} A \xi_{(i)} = N(\Lambda), \quad i = 1, 2, ..., s$$

On termine ici ce résumé de rappels. Il est loin d'être complet, mais on ne manquera pas d'en énoncer d'autres si c'est nécessaire.

Revenons à notre étude. Voronoï a démontré qu'en dimension n, il n'y a qu'un nombre fini de réseaux parfaits à similitude près. Leur dénombrement a été fait jusqu'en dimension 7 :

C'est ainsi qu'on a le tableau suivant :

dimension n	1	2	3	4	5	6	7	8
nombre de réseaux parfaits à équivalence près	1	1	1	2	3	7	33	?

Pour les dimensions 1, 2, 3, 4, 5, on doit essentiellement les résultats à Korkine et Zolotareff (1872-1877, c.f.[1]); pour la dimension 6 c'est à Barnes (1957, c.f. [2]); en dimension 7, il faut citer Stacey(1976, c.f. [3]), et Jaquet(1990, c.f. [4]).

Pour la dimension $n \geqslant 8$ on ne connaissait que très peu de réseaux parfaits, et les méthodes de calcul deviennent trop lourdes.

L'objet de ce travail est d'en donner un catalogue pour la dimension 8, en se limitant à ceux qui sont au-dessus des 33 réseaux parfaits existants en dimension 7.

1. Réseaux à section hyperplane donnée

Nous allons aborder maintenant le coeur du sujet.

Soit E un espace euclidien de dimension n. On considère un réseau Λ_0 de dimension n-1, inclus dans E, $S = S(\Lambda_0)$ l'ensemble de ses vecteurs minimaux, et H l'hyperplan de E engendré par Λ_0 .

Notons $\mathfrak{R}$ l'ensemble des réseaux Λ de E de même norme m que Λ_0

$$\text{(i.e : } \quad N(\Lambda) = N(\Lambda_0) = m), \text{ et tels que } \quad \Lambda \cap H = \Lambda_0.$$

Il est clair que l'on a $S_0 \subset S(\Lambda)$ (ensemble des vecteurs minimaux de Λ).

• **Problème** :

On étudie les réseaux Λ de $\mathfrak{R}$ qui réalisent un maximum local de la fonction d'Hermite $\gamma(\Lambda)$ dans $\mathfrak{R}$ (on rappelle que $\gamma(\Lambda) = \frac{N(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}}$).

Cette notion est stable par les isométries $f \in O(E)$, qui conservent la famille $\mathfrak{R}$, c'est-à-dire qui vérifient $f(\Lambda_0) = \Lambda_0$.

• **Description de $\mathfrak{R}$** :

D'abord une remarque : Soit Λ' un élément de $\mathfrak{R}$; on a $\Lambda' \cap H = \Lambda_0$; on montre facilement que le $\mathbb{Z}$-module de type fini $Q = \frac{\Lambda'}{\Lambda' \cap H}$ est sans torsion, donc libre avec une base $\{\bar{e'_n}\}$.

En effet : soit $\bar{x} \in \frac{\Lambda'}{\Lambda' \cap H}$, et soit $n \in \mathbb{Z}$, $n \neq 0$ tel que $n\bar{x} = \bar{0}$. On a :
$n\bar{x} = \bar{0} \Rightarrow nx \in \Lambda' \cap H = \Lambda_0 \Rightarrow nx \in H \Rightarrow x \in H \Rightarrow x \in \Lambda' \cap H \Rightarrow \bar{x} = \bar{0}$.
$Q = \frac{\Lambda'}{\Lambda \cap H}$ est bien sans torsion.
On arrive ainsi à la conclusion suivante :

Si $\mathfrak{B}_0 = \{e_1, e_2, ..., e_{n-1}\}$ *est une base de* Λ_0, *on peut la compléter en une base* $\{e_1, e_2, ..., e_{n-1}, e'_n\}$ *de* Λ'.

Désormais, posons Λ un élément *fixé* de $\mathfrak{R}$, et $\mathfrak{B} = \{e_1, e_2, ..., e_{n-1}, e_n\}$ une base de Λ complétant $\mathfrak{B}_0$. Caractérisons maintenant les éléments de $\mathfrak{R}$ relativement à certains éléments u de Gl(E) (groupe linéaire de E).

Pour ne pas alourdir certaines expressions dans les démonstrations, on conviendra d'écrire parfois uΛ au lieu de $u(\Lambda)$; de même qu'on écrira indifféremment S_0 pour $S(\Lambda_0)$ et S pour $S(\Lambda)$.

1.1 Proposition.
Soit le groupe $G = \{u \in Gl(E) |\ u|_H = Id_H\}$.
Alors : $\mathfrak{R} = \{u(\Lambda), u \in G, N(u\Lambda) = m\}$.

Démonstration.
Notons $\mathfrak{R}' = \{u\Lambda, u \in G, N(u\Lambda) = m\}$.
- On a $\mathfrak{R}' \subset \mathfrak{R}$.
En effet, u étant un élément de $Gl(E), u\Lambda$ est bien un réseau de E. Reste à montrer que $u\Lambda$ est dans $\mathfrak{R}$, c'est-à-dire que $u\Lambda \cap H = \Lambda_0$.
Montrons $u\Lambda \cap H \subset \Lambda_0$:
Soit $x \in u\Lambda \cap H$. On a x=u(y) avec $y \in \Lambda$,donc $u^{-1}(x) = y$; comme $u^{-1} \in G$ et que x appartient aussi à H, on a x=y donc $x \in \Lambda$. D'où $x \in \Lambda \cap H = \Lambda_0$.
L'inclusion $\Lambda_0 \subset (u\Lambda \cap H)$ est évidente :
Soit $x \in \Lambda_0$. Comme $\Lambda_0 = H \cap \Lambda, x$ appartient à Λ et à H, donc $u(x) = x \ \ (u \in G)$, d'où $x \in u\Lambda_0$.
Donc $x \in u\Lambda \cap H$.
- Réciproquement : a-t-on $\mathfrak{R} \subset \mathfrak{R}'$?
Soit $\Lambda' \in \mathfrak{R}$. D'après ce qui précède, Λ' admet une base $\mathfrak{B}'$ de la forme

$$\mathfrak{B}' = \{e_1, e_2, ..., e_{n-1}, e'_n\}.$$

Définissons l'application linéaire u par :

$$\begin{aligned} u(e_i) &= e_i, \quad 1 \leqslant i \leqslant n-1 \\ u(e_n) &= e'_n \end{aligned}$$

Alors u est dans G; de plus $u\Lambda$ est le réseau de base $\mathfrak{B}' = u(\mathfrak{B})$, c'est donc Λ'.
Donc Λ' est dans $\mathfrak{R}'$ puisque $N(\Lambda') = m$.
c.q.f.d.

Les matrices de Gram des réseaux Λ_0, Λ, et $u\Lambda$ dans $\mathfrak{R}$ se noteront :

$\bullet A_0 = Gram(\Lambda_0, \mathfrak{B}_0) = (e_i.e_j)_{\substack{1 \leq i \leq n-1 \\ 1 \leq j \leq n-1}}$,

$$\bullet A = Gram(\Lambda, \mathfrak{B}) = (e_i.e_j)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} = \left(\begin{array}{ccc|c} & & & e_1.e_n \\ & & & e_2.e_n \\ & A_0 & & \cdots \\ & & & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ e_n.e_1 & \cdots & \cdots & e_n.e_n \end{array}\right) ,$$

$$\bullet A' = Gram(u\Lambda, u\mathfrak{B})u \in G = \left(\begin{array}{ccc|c} & & & e_1.e'_n \\ & & & e_2.e'_n \\ & A_0 & & \cdots \\ & & & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ e'_n.e_1 & \cdots & \cdots & e'_n.e'_n \end{array}\right) .$$

Les matrices A et A' ont toutes les deux le bloc A_0 au même endroit. On dira d'une matrice ayant cette forme, qu'elle a un *coin* A_0.

2. Réseaux $\mathfrak{R}$-parfaits

On suppose ici que $\Lambda \in \mathfrak{R}$ réalise un maximum local pour la fonction γ. Étudions une propriété de ses vecteurs minimaux.

2.1 Notation :
On note :
a)$\mathcal{S}_H$ le sous-espace des endomorphismes symétriques v de E tels que $v(H) \subset H^\perp$
b)$\mathcal{S}_H^+$ le sous-ensemble des endomorphismes v de $\mathcal{S}_H$ à valeurs propres strictement positives.

2.2 Proposition.
1) Soit $u \in G$. Alors $v = {}^tuu - Id \in \mathcal{S}_H$.
2)Réciproquement : si $v \in \mathcal{S}_H$ et si $Id + v \in \mathcal{S}_H^+$, alors $\exists\ u \in G$ tel que ${}^tuu = Id + v$.

Démonstration. 1) :
a) Soit $u \in G$ et $v = {}^tuu - Id$. Montrons que v est symétrique. On a :

$${}^t({}^tuu - Id) = {}^t({}^tuu) - {}^tId = {}^tu\ {}^{tt}u - Id = {}^tuu - Id.$$

b)Montrons $v(H) \subset H^\perp$: soit $x \in H$, $y \in H$. On a :

$$\begin{aligned} v(x).y = ({}^tuu - Id)(x).y = ({}^tuu(x) - x).y = {}^tuu(x).y - x.y \\ = u(x).u(y) - x.y = x.y - x.y = 0 \end{aligned}$$

c.q.f.d

2)
Id+v possède des valeurs propres réelles strictement positives, d'après la définition de $\mathcal{S}_H^+$. Il existe donc un endomorphisme symétrique w à valeurs propres strictement positives tel que $w^2 = Id + v$. Soit $\{\varepsilon_1, \varepsilon_2, ..., \varepsilon_{n-1}\}$, une base orthonormée de H complétée en une base $\{\varepsilon_1, \varepsilon_2, ..., \varepsilon_{n-1}, \varepsilon_n\}$ orthonormée de E.

Définissons un automorphisme $g : E \to E$ par $g(\varepsilon_i) = w(\varepsilon_i)\ \forall\ i = 1, 2, ..., n-1$ et $g(\varepsilon_n) = u_n$, u_n vecteur de norme 1 orthogonal à tous les $w(\varepsilon_i)$ pour i = 1, 2, ..., n-1.

La famille $\{w(\varepsilon_1),\ w(\varepsilon_2),\ ...,\ w(\varepsilon_{n-1}),\ u_n\}$ est orthonormale.
En effet, pour $i, j \leq n-1$,

$$\begin{aligned} w(\varepsilon_i).w(\varepsilon_j) &= \varepsilon_i.w^2(\varepsilon_j) \quad (\text{ car w symétrique}) \\ &= \varepsilon_i.(Id+v)(\varepsilon_j) = \varepsilon_i.[\varepsilon_j + v(\varepsilon_j)] = \varepsilon_i.\varepsilon_j + \varepsilon_i.v(\varepsilon_j) \\ &= \varepsilon_i.\varepsilon_j \quad (\text{car } v(H) \subset H^\perp) \end{aligned}$$

Montrons que $g \in O(E)$. Soient x ,y dans E.
$x = \lambda_1\varepsilon_1 + \lambda_2\varepsilon_2 + ... + \lambda_n\varepsilon_n$
$y = \beta_1\varepsilon_1 + \beta_2\varepsilon_2 + ... + \beta_n\varepsilon_n$
$x.y = \lambda_1\beta_1 + \lambda_2\beta_2 + ... + \lambda_n\beta_n$
$g(x) = \lambda_1 w(\varepsilon_1) + \lambda_2 w(\varepsilon_2) + ... + \lambda_n w(\varepsilon_n)$
$g(y) = \beta_1 w(\varepsilon_1) + \beta_2 w(\varepsilon_2) + ... + \beta_n w(\varepsilon_n)$
$g(x).g(y) = \lambda_1\beta_1 + \lambda_2\beta_2 + ... + \lambda_n\beta_n$
D'où $g(x).g(y) = x.y$
Donc g^{-1} aussi est dans O(E).
${}^t(g^{-1}w)g^{-1}w = {}^tw{}^tg^{-1}g^{-1}w = {}^twgg^{-1}w = {}^tww = w^2 = Id + v$
g^{-1} est dans G :
Soit $x \in H; x = \lambda_1\varepsilon_1 + \lambda_2\varepsilon_2 + ... + \lambda_n\varepsilon_n$
$g^{-1}w(x) = \lambda_1 g^{-1}w(\varepsilon_1) + \lambda_2 g^{-1}w(\varepsilon_2) + ... + \lambda_n g^{-1}w(\varepsilon_{n-1}) = \lambda_1 g^{-1}g(\varepsilon_1) + \lambda_2 g^{-1}g(\varepsilon_2) + ... + \lambda_n g^{-1}g(\varepsilon_{n-1}) = \lambda_1\varepsilon_1 + \lambda_2\varepsilon_2 + ... + \lambda_n\varepsilon_{n-1}$
$= x$

On prendra $f = g^{-1}$, et alors $u = g^{-1}w$
c.q.f.d

2.3 Définition.

$\Lambda \in \mathfrak{R}$ *est dit* $\mathfrak{R}$*-parfait si on a l'implication suivante :*

$$\left.\begin{array}{l} v \in \mathcal{S}_H \\ v(x).x = 0 \forall\ x \in S(\Lambda) \end{array}\right\} \quad \Rightarrow v = 0$$

2.4 Remarques.

1)Si l'on substitue dans 2.3, à $\mathcal{S}_H$ l'ensemble de tous les endomorphismes symétriques de E, on retrouve la notion classique de *perfection* introduite par Korkine et Zolotareff. De plus, tout réseau parfait appartenant à $\mathfrak{R}$ est $\mathfrak{R}$-parfait.
2)La condition qui définit la $\mathfrak{R}$-perfection peut s'énoncer ainsi :

les formes linéaires $\varphi_x : v \to v(x).x$ *sur* S_H *engendrent le dual* $(S_H)^*$ *de* S_H.
3)Seuls interviennent les $x \in S - S_0$, car si $x \in H$, $v(x).x = 0$ pour tout $v \in S_H$.
On peut donc dans 2.4, remplacer " $\forall\ x \in S(\Lambda)$ " par " $\forall\ x \in S(\Lambda) - S(\Lambda_0)$ ".
4)*Les isométries de* E *qui stabilisent le réseau* Λ_0 *(section des réseaux de* $\Re$ *par* H*), conservent cette notion de* $\Re$*-perfection.*

En effet soit $\Lambda \in \Re$ un réseau $\Re$-parfait, et $f \in O(E)$ tel que $f(\Lambda_0) = \Lambda_0$. Pour $v \in S_H$, on a ${}^t fvf \in S_H$; (pour $h \in H, h' \in H$, *on a* : ${}^t fvf(h).h' = vf(h).f(h') = 0$ car f stabilise H).

Comme f est une isométrie, il est clair que $S(f(\Lambda)) = f(S(\Lambda))$.
Montrons que $f(\Lambda)$ est $\Re$-parfait :

soit $v \in S_H$. D'après ce qui précède on a les équivalences :

$$vy.y = 0\ \forall\ \ y \in S(f(\Lambda)) \Leftrightarrow vf(x).f(x) = 0\ \forall\ \ x \in S(\Lambda) \Leftrightarrow {}^t fvf(x).x = 0\ \forall\ \ x \in S(\Lambda).$$

Puisque $tfvf \in S_H$, et puisque Λ est $\Re$-parfait on en déduit ${}^t fvf = 0$, donc $v = 0$.

2.5 Théorème.
Si $\Lambda \in \Re$ *réalise un maximum local de* γ, *alors* Λ *est* $\Re$*-parfait.*

Pour la démonstration on utilisera le lemme suivant :

2.6 Lemme.
Si on pose ${}^t uu = Id + \varepsilon v, \varepsilon > 0$ *assez petit, alors on a les équivalences :*
a) $det({}^t uu) = 1 \Leftrightarrow u \in O(E) \Leftrightarrow v = 0$
b) $det({}^t uu) > 1 \Leftrightarrow Tr(v) > 0$

Soit $P_v(X) = X^n - T_1 X^{n-1} + T_2 X^{n-2} + ... + (-1)^n T_n$ le polynôme caractéristique de v, où $T_1 (= Tr(v)), T_2, ..., T_n$ sont les fonctions symétriques élémentaires des valeurs propres $\lambda_1, \lambda_2, ..., \lambda_n$ (non nécéssairement distinctes) de v.

De l'égalité $\det(XId - v) = X^n - T_1 X^{n-1} + ... + (-1)^n T_n$ on déduit par division par X^n,

$$\det(Id - \frac{1}{X}v) = 1 - T_1 \frac{1}{X} + T_2 \frac{1}{X^2} + ... + (-1)^n \frac{T_n}{X^n}.$$

D'où en posant $\varepsilon = -\frac{1}{X}$:

$$\det(Id + \varepsilon v) = 1 + T_1\varepsilon + T_2\varepsilon^2 + ... + T_n\varepsilon^n \tag{1}$$

$$\det(Id + \varepsilon v) = 1 + T_1\varepsilon + T_2\varepsilon^2 + o(\varepsilon^2) \tag{2}$$

Démonstration.

a)
On a évidemment

$$u \in O(E) \Longleftrightarrow {}^t uu = Id \Longleftrightarrow v = 0.$$

Supposons $\det({}^t uu) = 1$. D'après (1), on a $T_1, T_2, ..., T_n$ nuls. Donc $P_v(X) = X^n$ et comme v est symétrique (donc diagonalisable) v=0.
Réciproquement : si $v = 0, {}^t uu = Id$, donc $\det({}^t uu) = 1$

b)
Supposons $\det({}^t uu) > 1$, et montrons $T_1 > 0$.
Si $T_1 \leq 0$:
-) $T_1 < 0$: d'après (2), $\det(Id + \varepsilon v) = \det({}^t uu) < 1$.
-) $T_1 = 0$, alors on peut montrer que $T_2 < 0$:
$2T_2 = 2\sum_{i<j} \lambda_i \lambda_j = (\lambda_1 + ... + \lambda_n)^2 - ({\lambda_1}^2 + ... + {\lambda_n}^2) = -({\lambda_1}^2 + ... + {\lambda_n}^2)$.
Comme ${}^t uu$ est symétrique, donc v aussi, les λ_i sont reéls. Donc $\sum \lambda_i^2 \geqslant 0$.
$\sum \lambda_i^2 = 0$ entraînerait $\lambda_i = 0\ \forall i$. Donc v=0, d'où d'après a) $\det({}^t uu) = 1$ ce qui est exclu.
On a donc $\sum \lambda_i^2 > 0$, donc $T_2 < 0$. La formule (2) devient :

$$\det(Id + \varepsilon v) = 1 + \varepsilon^2 T_2 + o(\varepsilon^2) \text{ avec } T_2 < 0$$

D'où $\det({}^t uu) < 1$ pour ε assez petit. Ce qui est absurde.
c.q.f.d.

Démonstration du théorème 2.5 :

Soit Λ un réseau de $\mathfrak{R}$ réalisant un maximum local de γ. Supposons v dans $\mathcal{S}_H$ tel que $\forall x \in S(\Lambda),\ v(x).x = 0$. Montrons que $v = 0$.
Supposons que $v \neq 0$. Alors pour $\varepsilon > 0$, assez petit, $Id + \varepsilon v$ a ses valeurs propres positives (si $\lambda_1, \lambda_2, ..., \lambda_n$ désignent les valeurs propres de v, celles de $Id + \varepsilon v$ sont $1 + \varepsilon\lambda_1, 1 + \varepsilon\lambda_2, ..., 1 + \varepsilon\lambda_n$).
Par 2.3, $\exists\ u \in G$ tel que ${}^t uu = Id + \varepsilon v$
Considérons le réseau $u\Lambda$. On montre que $N(u\Lambda) = N(\Lambda)$:
Soit $x \in S$. On a :

$$N(u(x)) = u(x).u(x) = {}^t uu.x = (Id + \varepsilon v)(x).x = x.x + \varepsilon v(x).x = m$$

Or pour ε assez petit les vecteurs minimaux de $u\Lambda$ proviennent de ceux de Λ, c'est à dire $N(u\Lambda) = \min_{x \in S} N(u(x)) = m$.
Donc par 1.1, le réseau $u\Lambda$ est dans $\mathfrak{R}$.
Par ailleurs $\det(u\Lambda) = \det({}^t uu).\det(\Lambda)$: En effet, soit $\mathcal{E}$ une base orthonormée de E; on rappelle que $\det \Lambda = (\Delta\ (\Lambda))^2 = (\det_{\mathcal{E}} \mathfrak{B})^2$.
Alors $\det u\Lambda = (\det_{\mathcal{E}} u\mathfrak{B})^2$
$= (\det_{\mathcal{E}} \mathfrak{B}.(\det_{(\mathfrak{B})} u\mathfrak{B})^2$
$= (\det_{\mathcal{E}} \mathfrak{B})^2.(\det_{(\mathfrak{B})} u\mathfrak{B})^2$
$= \det \Lambda.(\det_{(\mathfrak{B})} u\mathfrak{B})^2$

$= (\det u)^2 . \det \Lambda$.

$$\gamma(u\Lambda) = \frac{m}{(\det u\Lambda)^{\frac{1}{n}}} = \frac{m}{(\det {}^t uu)^{\frac{1}{n}}(\det \Lambda)^{\frac{1}{n}}} = \frac{\gamma(\Lambda)}{(\det {}^t uu)^{\frac{1}{n}}}$$

Puisque $u\Lambda$ est dans $\mathfrak{R}$ et que $\gamma(\Lambda)$ est un maximum local dans $\mathfrak{R}$, on doit avoir :
$\gamma(u\Lambda) \leqslant \gamma(\Lambda)$ pour ε assez petit, c'est à dire $\det {}^t uu \geqslant 1$.
D'après 2.6, puisque $v \neq 0$, on a $\det {}^t uu > 1$ et alors $Tr(v) > 0$.
En résumé, tout $v \neq 0$ de $\mathcal{S}_H$ vérifiant $v(x).x = 0\ \forall x \in S(\Lambda)$ doit avoir $Tr(v) > 0$. Comme -v vérifie les mêmes hypothèses que v, on doit avoir à la fois Tr(v) et Tr(-v) positives strictement, ce qui est absurde.
c.q.f.d.

2.7 Théorème.

$$\left.\begin{array}{l} \Lambda_0\ parfait \\ \Lambda\ \mathfrak{R} - parfait \end{array}\right\} \quad \Rightarrow \Lambda\ parfait$$

Démonstration.

Notons $\mathcal{S}_0$ l'ensemble des $v \in End^s E$ tel que $v(H) \subset H$ *et* $v(H^\perp) = \{0\}$ et montrons qu'il est est supplémentaire de $\mathcal{S}_H$ dans $End^s E$.

Soit en effet $\mathcal{E} = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_{n-1}, \varepsilon_n\}$ une base orthonormée de E avec $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{n-1}$, dans H, et soient $v_0 \in \mathcal{S}_0$ et $w \in \mathcal{S}_H$.

Leurs matrices dans $\mathcal{E}$ sont de la forme :

$$mat(v_0, \mathcal{E}) = \left(\begin{array}{ccc|c} & & & 0 \\ & A_0 & & 0 \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ 0 & \cdots & \cdots & 0 \end{array}\right) \quad \text{et} \quad mat(w, \mathcal{E}) = \left(\begin{array}{ccc|c} & & & \lambda_1 \\ & 0 & & \lambda_2 \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ \lambda_1 & \cdots & \cdots & \lambda_n \end{array}\right),$$

où les λ_i sont dans $\mathbb{R}$ et A_0 est une matrice symétrique d'ordre n-1.
À partir de cette remarque on déduit facilement la démonstration du théorème :
Soit $v \in End^s(E)$ tel que $v(x).x = 0\ \forall\ x \in S(\Lambda)$. Montrons que $v = 0$.
On peut écrire d'après ce qui précède :

$$v = v_0 + w \text{ avec } w \in \mathcal{S}_H, \text{ et } v_0 \in \mathcal{S}_0.$$

Or par hypothèse $v(x).x = 0\ \forall x \in S(\Lambda)$; on en déduit pour tout $x \in S(\Lambda)$
$(v_0 + w)(x).x = 0$, c'est-à-dire $v_0(x).x + w(x).x = 0$. Ceci est vrai en particulier pour tout $x \in S(\Lambda_0)$.
Or pour un tel x, qui est dans H, on a $w(x) \in H^\perp$ (par définition de $\mathcal{S}_H$) donc en particulier $wx.x = 0\ \forall\ x \in S(\Lambda_0)$. D'où l'on déduit $v_0 x.x = 0\ \forall\ x \in S(\Lambda_0)$. Comme la restriction de v_0 à H est dans $End^s H$, la perfection de Λ_0 permet de conclure que cette restriction est nulle, donc aussi v_0.

On a donc $v = w$, d'où $wx.x = 0 \ \forall \ x \in S(\Lambda)$, ce qui implique $w = 0$ puisque Λ est $\mathfrak{R}$-parfait. Donc $v = 0$ et Λ est parfait.
c.q.f.d.

Remarque : Si l'on pose $\langle v, v' \rangle = Tr(vv') = Tr(v'v)$, on vérifie facilement que cela définit un produit scalaire dans $End^s E$ (voir §3).

Le sous-espace $\mathcal{S}_0$ de $End^s E$ est alors égal à ${\mathcal{S}_H}^{\perp}$, supplémentaire de $\mathcal{S}_H$ dans $End^s E$.

En effet, en gardant les notations précédentes, soient $w \in \mathcal{S}_H$ et $v \in End^s E$ de matrice (a_{ij}) dans $\mathcal{E}$. On a :
$\langle v, w \rangle = 2(a_{1n}\lambda_1 + a_{2n}\lambda_2 + ... + a_{(n-1)n}\lambda_{n-1}) + a_{nn}\lambda_n \ \forall \ (\lambda_1, \lambda_2, ..., \lambda_n) \in \mathbb{R}^n$.

D'où les équivalences :

$$v \in {\mathcal{S}_H}^{\perp} \Leftrightarrow \langle v, w \rangle = 0 \ \forall \ w \in \mathcal{S}_H \Leftrightarrow a_{1n} = a_{2n} = ... = a_{(n-1)n} = a_{nn} = 0 \Leftrightarrow v \in \mathcal{S}_0.$$

On a vu que seuls interviennent pour la $\mathfrak{R}$-perfection, les vecteurs minimaux de Λ qui sont hors de H. La caractérisation suivante précise leur rôle :

2.8 Théorème.
Soit $\Lambda \in \mathfrak{R}$. Alors :
Pour que Λ soit $\mathfrak{R}$-parfait il faut et il suffit que les vecteurs minimaux de Λ hors de H engendrent E.

Démonstration.
Soit $\mathcal{E} = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_{n-1}, \varepsilon_n\}$ une base orthonormée de E complétant une base orthonormée $\{\varepsilon_1, \varepsilon_2, ..., \varepsilon_{n-1}\}$ de H. Si $v \in \mathcal{S}_H$, on a vu que sa matrice est de la forme :

$$mat(v, \mathcal{E}) = \left(\begin{array}{ccc|c} & & & \lambda_1 \\ & & & \lambda_2 \\ & 0 & & \cdots \\ & & & \cdots \\ \hline \lambda_1 & \cdots & \cdots & \lambda_n \end{array}\right)$$

de sorte que pour x dans E, x s'écrivant $x = \sum_{i=1}^{n} \beta_{x,i}\varepsilon_i$, on a :

$\varphi_x(v) = v(x).x$, et après calcul

$$\varphi_x(v) = \beta_{x,n}(2\beta_{x,1}\lambda_1 + ... + 2\beta_{x,n-1}\lambda_{n-1} + \beta_{x,n}\lambda_n). \tag{3}$$

a)Condition nécessaire :
Supposons Λ $\mathfrak{R}$-parfait et montrons que les x en dehors de H engendrent E. En effet, sinon ils appartiendraient tous à un hyperplan d'équation

$$\alpha_1 X_1 + ... + \alpha_n X_n = 0$$

où les α_i ne sont pas tous nuls (les X_i étant les composantes de x suivant la base $(\varepsilon_i)_{1 \leqslant i \leqslant n}$).

Prenons v défini par la matrice suivante :

$$mat(v, \mathcal{E}) = \begin{pmatrix} & & & | & \frac{\alpha_1}{2} \\ & & & | & \frac{\alpha_2}{2} \\ & 0 & & | & \cdots \\ & & & | & \cdots \\ --- & --- & --- & | & \frac{\alpha_{n-1}}{2} \\ \frac{\alpha_1}{2} & \cdots & \cdots & \frac{\alpha_{n-1}}{2} & \alpha_n \end{pmatrix}$$

D'après la formule (3), on a $\varphi_x(v) = 0 \ \forall \ x \in S$, et pourtant $v \neq 0$; ce qui contredit l'hypothèse Λ $\mathfrak{R}$-parfait.

b)Condition suffisante :

Supposons que les x hors de H engendrent E, et montrons que Λ est $\mathfrak{R}$-parfait. S'il n'en était pas ainsi, il existerait un $v \in \mathcal{S}_H$, non nul tel que $\varphi_x(v) = 0 \ \forall \ x \in S$.

Si

$$mat(v, \mathcal{E}) = \begin{pmatrix} & & & | & \lambda_1 \\ & & & | & \lambda_2 \\ & 0 & & | & \cdots \\ & & & | & \cdots \\ --- & --- & --- & | & \cdots \\ \lambda_1 & \cdots & \cdots & & \lambda_n \end{pmatrix}$$

est la matrice de v dans la base $\mathcal{E}$, avec les λ_i non tous nuls, la formule (3) donne, pour $x = \sum \beta_{x,i} \ \varepsilon_i \in S - H$, où $\beta_{x,n}$ n'est pas nul (x n'appartient pas à H) :

$$2\beta_{x,1}\lambda_1 + ... + 2\beta_{x,n-1}\lambda_{n-1} + \beta_{x,n}\lambda_n = 0 \quad .$$

Ainsi, tous les vecteurs minimaux hors de H appartiendraient à l'hyperplan de E d'équation $2\lambda_1 X_1 + ... + 2\lambda_{n-1}X_{n-1} + \lambda_n X_n = 0$ ce qui contredit l'hypothèse.

c.q.f.d.

De 2.7 et 2.8 résulte immédiatement un critère de perfection :

2.9 Corollaire. *Soit Λ_0 un réseau parfait d'un hyperplan H de E, et soit Λ un réseau de E de même norme, et tel que $\Lambda \cap H = \Lambda_0$. Alors pour que Λ soit parfait, il faut et il suffit que ses vecteurs minimaux hors de H engendrent E.*

Voronoï a montré qu'il existe un nombre fini de réseaux parfaits (à similitude près) en dimension et norme données. Il a de plus mis au point un algorithme qui permet de les déterminer tous à partir de l'un d'entre eux. Dans la pratique la manipulation se fera avec les matrices de Gram.

Chapitre II

THÉORÈMES À LA " VORONOÏ "

3. Espace et domaine de Voronoï

On sait que les valeurs propres λ_i d'une matrice réelle symétrique A sont réelles, et que les valeurs propres de A^2 sont les ${\lambda_i}^2$.

Partant de cette remarque, on démontre facilement que dans l'espace vectoriel des matrices carrées symétriques réelles d'ordre n, l'application :

$$(A, B) \mapsto Trace(A, B) = Tr(AB) = Tr(BA)$$

est un produit scalaire qu'on notera $\langle A, B \rangle$.

3.1 Définition.

On appelle espace de Voronoï l'espace euclidien Vor des matrices réelles symétriques d'ordre n muni du produit scalaire $\langle A, B \rangle = Tr(A, B)$.

Cet espace euclidien Vor est de dimension $\dfrac{n(n+1)}{2}$.

3.2 Représentation dans Vor d'un vecteur de $\mathbb{R}^n$.

Tout $\xi = \begin{pmatrix} \xi_1 \\ \vdots \\ \vdots \\ \xi_n \end{pmatrix}$ de $\mathbb{R}^n$ peut être représenté dans Vor par la matrice

$$X = \xi^t \xi = \begin{pmatrix} {\xi_1}^2 & \xi_1\xi_2 & \dots & \xi_1\xi_n \\ \xi_2\xi_1 & {\xi_2}^2 & \dots & \xi_2\xi_n \\ \vdots & \vdots & \ddots & \vdots \\ \xi_n\xi_1 & \xi_n\xi_2 & \dots & {\xi_n}^2 \end{pmatrix},$$

et il est facile de voir que dans Vor, $\langle A, X\rangle = {}^t\xi A\xi$.

Revenons à la notion de perfection de réseau, et donnons une autre interprétation à l'aide de matrice A symétrique réelle d'ordre n.

3.3 Définition.
La matrice A est dite parfaite si elle correspond à une matrice de Gram d'un réseau parfait Λ *dans une base du réseau.*

Cette notion est évidemment stable par équivalence. Pour exprimer cette condition, nous représentons un élément x de E dans la base $\mathfrak{B} = \{e_1, e_2, ..., e_n\}$ du réseau par la matrice $X = \xi {}^t\xi \in Vor$ comme il a été dit dans 3.2 (ξ est la matrice unicolonne représentant x dans $\mathbb{R}^n$) et un endomorphisme symétrique v de E par la matrice

$$M = (v(e_i).e_j) = (v(e_j).e_i) \in Vor$$

On a alors :

$$vx.x = {}^t\xi M\xi = Tr({}^t\xi M\xi) = Tr(({}^t\xi M)\xi) = Tr(\xi({}^t\xi M)) = Tr((\xi {}^t\xi)M) = \langle X, M\rangle$$

[Noter que lorsque $v = Id$, et donc $M = A$, on retrouve la formule de 3.2]
La condition $vx.x = 0$ exprime donc que $X = \xi {}^t\xi$ est orthogonal à M dans Vor.

3.4 Proposition.
La matrice A est parfaite si et seulement si les matrices X (les X représentant dans Vor les vecteurs minimaux de Λ*) engendrent l'espace Vor.*

Démonstration.
La perfection de A au sens classique (c.f. 2.3 et 2.4), signifie que le sous-espace de Vor orthogonal à l'espace engendré par les $X = \xi {}^t\xi$ lorsque x décrit $S(\Lambda)$ est nul; donc les matrices X lorsque x décrit $S(\Lambda)$ engendrent Vor.
c.q.f.d.

Voronoï a alors associé à chaque matrice parfaite un cône convexe d'intérieur non vide:

3.5 Définition.
Notons $X_1, X_2, ..., X_s$ *les représentations dans Vor des vecteurs minimaux de A. On appelle domaine de Voronoï* $\mathfrak{D}_A$*, de la matrice A, l'enveloppe convexe des demi-droites engendrées par les* $(X_i)_{i=1,2,...,s}$*, i.e :*

$$\mathfrak{D}_A = \{\sum_{i=1}^{s} \lambda_i X_i,\ \lambda_i \geqslant 0,\ \lambda_i \in \mathbb{R}\}$$

On va voir par la suite que ces domaines constituent un *"pavage"* de l'espace de Voronoï.

4. Contiguïté de réseaux parfaits

Définissons d'abord la contiguïté de deux matrices parfaites :

Soit A une matrice parfaite de minimum m(A), S(A) l'emsemble des matrices $X = \xi {}^t\xi$ représentant ses vecteurs minimaux dans l'espace de Voronoï, et $\mathfrak{D}_A$ le domaine de Voronoï de A. Comme A est parfaite, $\mathfrak{D}_A$ est de dimension $\frac{n(n+1)}{2}$.

On considère une face d'appui $\mathfrak{H}$ hyperplane de $\mathfrak{D}_A$, et B un *vecteur de face* correspondant à $\mathfrak{H}$, i.e :

$$\langle B, X\rangle = 0 \ \forall\ X \in \mathfrak{H} \text{ et } \langle B, X\rangle\ > 0\ \forall X \in S(A) - \mathfrak{H}.$$

On considère alors pour $\theta > 0$, $A_\theta = A + \theta B \in$ Vor .

Pour tout $X = \xi {}^t\xi$, on a $\langle A_\theta, X\rangle = \langle A, X\rangle + \theta\langle B, X\rangle$; donc :

$$\begin{cases} - \text{ si } X \in \mathfrak{H},\ \langle A_\theta, X\rangle = m(A) \\ - \text{ si } X \in S(A) - \mathfrak{H},\ \langle A_\theta, X\rangle > m(A). \end{cases}$$

(Voir figure 2 de l'annexe I).

On démontre que (c.f [8] ou [9] ou [10]) :

l'ensemble $\{\theta \mid \langle A_\theta, X\rangle\ = m(A)\}$ *est borné et que pour* $\theta_0 = sup\{\theta\}$, *la matrice* A_{θ_0} *est parfaite :*

en effet, il existe $X_0 \notin \mathfrak{H}$ tel que pour $\theta > \theta_0$, $\langle A_\theta, X_0\rangle\ < m(A)$ et $\langle A_\theta, X_0\rangle\ = m(A)$, donc $X_0 \in S(A_{\theta_0})$ qui engendre alors Vor (car $S(A_{\theta_0}) \supset (\mathfrak{H} \cup \{X_0\})$

D'où la notion de contiguïté que nous allons définir en donnant quelques propriétés.

4.1 Définition.

La matrice parfaite A_{θ_0} *(de même norme que A) donnée ci-dessus, s'appelle la contiguë de A par la face perpendiculaire à B (ou contiguë de A par la face B (abus de langage)).*

• Voronoï (1908 c.f. [8]) a démontré que le graphe de contiguïté ainsi défini est connexe. Par ailleurs *la relation de contiguïté est compatible avec l'équivalence* (i.e si A_{θ_0} est la contiguë de A par la face de $\mathfrak{D}_A$ perpendiculaire à B, ${}^tPA_{\theta_0}P$ est la contiguë de $A' = {}^tPAP$ par la face de $\mathfrak{D}_A$ perpendiculaire à ${}^tPBP$); et si l'on supprime à chaque étape les matrices équivalentes à une matrice déja rencontrée, le graphe ainsi obtenu est fini et donne (à équivalence près), toutes les matrices parfaites de dimension n.

Voronoï lui-même a retrouvé par cet algorithme les listes (à équivalence près) de formes quadratiques parfaites en $dim \leqslant 5$ dues à Korkine-Zolotareff; et Barnes a repris en 1956

ces méthodes pour établir la liste des 7 formes parfaites en dimension 6. Jaquet vient de résoudre le cas de la dimension 7, et a établi que la liste des 33 formes établies par Stacey est complète (c.f. [4],c)

La suite du paragraphe est consacrée à une adaptation de cet algorithme pour établir la liste des formes quadratiques parfaites de dimension 8 qui prolongent chacune des 33 formes à part les formes O_7, V_7, Z_7 (dans la terminologie de Korkine-Zolotareff, qui correspondent aux systèmes de racines $\mathbb{A}_7, \mathbb{D}_7, \mathbb{E}_7$). On expliquera au §11 pourquoi les réseaux de racines n'ont pas été traités.

4.2 Interprétation de l'ensemble $\mathfrak{R}$ dans l'espace de Voronoï.

Reprenons l'ensemble $\mathfrak{R}$ défini au §1, et faisons un certain nombre de remarques.

On note Vor_0 l'espace de Voronoï de $dim \frac{(n-1)n}{2}$, plongé dans l'espace Vor (de dimension $\frac{n(n+1)}{2}$) de la façon suivante :

ses éléments sont de la forme

$$\left(\begin{array}{ccc|c} & & & 0 \\ & & & 0 \\ & * & & \cdots \\ & & & \cdots \\ \hline\hline \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 \end{array}\right) ,$$

où le coin (*) représente une matrice symétrique réelle d'ordre n-1.

C'est un sous-espace de Vor de codimension n. Son supplémentaire orthogonal dans Vor est l'espace des matrices symétriques de la forme

$$\left(\begin{array}{ccc|c} & & & a_1 \\ & & & a_2 \\ & 0 & & \cdots \\ & & & \cdots \\ \hline\hline \cdots & \cdots & \cdots & \cdots \\ a_1 & \cdots & \cdots & a_n \end{array}\right)$$

de dimension n.

(Compte tenu des dimensions, il suffit de vérifier que la trace du produit de deux matrices ayant chacune les formes précitées, est nulle).

On se donne maintenant un réseau parfait Λ_0 de dimension n-1 rapporté à une base $\{e_1, e_2, ..., e_{n-1}\}$, de matrice de Gram A_0 appartenant à Vor_0. Les réseaux de $\mathfrak{R}$ ont dans une base $\mathfrak{B} = \{e_1, e_2, ..., e_n\}$ convenable une matrice de Gram avec un *coin* A_0, c'est-à-dire de la forme

$$A = \left(\begin{array}{ccc|c} & & & a_1 \\ & A_0 & & a_2 \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ a_1 & \cdots & \cdots & a_n \end{array}\right) \qquad (c.f.\S 1).$$

Soit $\mathfrak{B}' = \{e'_1, e'_2, ..., e'_n\}$ une autre base du réseau Λ, avec $\{e'_1, e'_2, ..., e'_{n-1}\}$ base de Λ_0. La matrice de passage $P \in Gl_n(\mathbb{Z})$ de $\mathfrak{B}$ à $\mathfrak{B}'$ est de la forme

$$(1) \qquad P = \left(\begin{array}{ccc|c} & & & p_1 \\ & P_0 & & p_2 \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ 0 & \cdots & \cdots & p_n \end{array}\right) \quad ,$$

où $P_0 \in Gl_{n-1}(\mathbb{Z})$ est la matrice de passage de $\{e_1, e_2, ..., e_{n-1}\}$ à $\{e'_1, e'_2, ..., e'_{n-1}\}$ et où les p_i sont des entiers, et $p_n = \pm 1$ (car $\det P = \det P_0 . p_n$).

4.3 Définition.

On dira que deux matrices de Gram

$$A = \left(\begin{array}{ccc|c} & & & * \\ & A_0 & & * \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ * & \cdots & \cdots & * \end{array}\right) \quad et \quad A' = \left(\begin{array}{ccc|c} & & & * \\ & A_0 & & * \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ * & \cdots & \cdots & * \end{array}\right)$$

sont A_0-équivalentes s'il existe P de la forme (1) tel que : $A' = {}^tPAP$.

Ainsi au réseau Λ est associée la classe de A_0-équivalence de A.

Soit maintenant $f \in O(E)$ une isométrie telle que $f(\Lambda_0) = \Lambda_0$. Dans la base $f(\mathfrak{B})$, le réseau $f(\Lambda)$ a pour matrice $A = Gram(\Lambda, \mathfrak{B})$ (c.f. §1), donc on obtient :

une bijection entre classes d'équivalence de réseaux par les isométries conservant Λ_0, et classes de A_0-équivalence de matrices de Gram.

Soit Λ un réseau $\mathfrak{R}$-parfait de matrice de Gram

$$A = \left(\begin{array}{ccc|c} & & & \alpha_1 \\ & & & \alpha_2 \\ & A_0 & & \cdots \\ & & & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ \alpha_1 & \cdots & \cdots & \alpha_n \end{array}\right) .$$

A est parfaite (c.f. 2.7).

On note

$$\mathfrak{D}_A = \{\sum_{i=1}^{s} \lambda_i X_i,\ \lambda_i \geqslant 0\}$$

son domaine de Voronoï , les X_i étant les représentations dans Vor des vecteurs mininmaux de A.

Les matrices parfaites $A_\theta = A + \theta B$ contiguës de A et qui représentent des réseaux de $\mathfrak{R}$ sont de la forme

$$\left(\begin{array}{ccc|c} & & & b_1 \\ & & & b_2 \\ & A_0 & & \cdots \\ & & & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ b_1 & \cdots & \cdots & b_n \end{array}\right) .$$

Par différence on voit que les vecteurs de face de $\mathfrak{D}_A$ à considérer sont de la forme

$$B = \left(\begin{array}{ccc|c} & & & a_1 \\ & & & a_2 \\ & 0 & & \cdots \\ & & & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ a_1 & \cdots & \cdots & a_n \end{array}\right) ,$$

c'est à dire sont dans $Vor_0{}^{\perp}$ (d'après 4.2);

autrement dit les faces d'appui de $\mathfrak{D}_A$ que nous considérons sont celles qui contiennent Vor_0.

Ainsi nous sommes amenés à travailler dans un sous-espace de dimension n de l'espace de Voronoï (de dimension $\dfrac{n(n+1)}{2}$*).*

Précisons la correspondance :

Soit S ($\subset \mathbb{Z}^n$) l'ensemble des vecteurs minimaux $\xi = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ de A. Quitte à remplacer

ξ par $-\xi$, on suppose $\xi_n \geqslant 0$. Pour $\xi_n = 0$, on trouve l'ensemble S_0 des vecteurs minimaux de A_0.

4.4 Proposition.
Soit

$$B = \left(\begin{array}{ccc|c} & & & a_1 \\ & 0 & & a_2 \\ & & & \cdots \\ & & & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ a_1 & \cdots & \cdots & a_n \end{array}\right),$$

un vecteur non nul de $Vor_0{}^{\perp}$.
Pour que B soit un vecteur de face du domaine $\mathfrak{D}_A$, il faut et il suffit que l'hyperplan H_B de $\mathbb{R}^n$ d'équation

$$2a_1x_1 + 2a_2x_2 + \ldots + 2a_{n-1}x_{n-1} + a_nx_n = 0$$

soit engendré par des vecteurs minimaux ξ de A, et que tous les vecteurs minimaux de A soient d'un même côté de H_B.

Démonstration.
Pour $\xi \in S$, on note $X = \xi^t\xi$; B est un vecteur de face de $\mathfrak{D}_A$ si et seulement si l'hyperplan $B^{\perp}$ est engendré par les X qu'il contient et si l'on a $\langle B, X\rangle \geqslant 0\ \forall\ X$ représentant un vecteur minimal de A. L'hyperplan $B^{\perp}$ de Vor contient déja les représentations X des vecteurs de S_0.
Puisque A_0 est parfaite, ces vecteurs engendrent Vor_0 (qui est de codimension n-1 dans $B^{\perp}$).
Pour que $B^{\perp}$ soit une face de $\mathfrak{D}_A$ il faut et il suffit que les représentations X des vecteurs de $S - S_0$ contenues dans $B^{\perp}$ engendrent un sous-espace de dimension n-1 supplémentaire de Vor_0 (dans $B^{\perp}$).
Pour $\xi = \begin{pmatrix} \xi_1 \\ \vdots \\ \vdots \\ \xi_n \end{pmatrix}$ dans S, on a $\langle B, X\rangle = \xi_n(2a_1\xi_1 + \ldots + 2a_{n-1}\xi_{n-1} + a_n\xi_n)$ de sorte que $X \in B^{\perp}$ équivaut à : $\xi_n = 0$ ($i.e\ \xi \in S_0$) ou bien $2a_1\xi_1 + \ldots + 2a_{n-1}\xi_{n-1} + a_n\xi_n = 0$ (i.e ξ appartient à l'hyperplan H_B de $\mathbb{R}^n$).
Soit $S_1 \subset (S - S_0)$ un système de n-1 vecteurs minimaux de H_B. Le sous-espace de $B^{\perp}$ engendré par les $(\xi^t\xi)_{\xi\in S_1}$ est en somme directe avec Vor_0 si et seulement si le système S_1 est de rang n-1 (i.e : est une base de H_B). En effet les conditions suivantes sont équivalentes pour $(\lambda_\xi)_{\xi\in S_1} \in \mathbb{R}^{n-1}$:

(1) $$\sum_{\xi\in S_1} \lambda_\xi \xi^t\xi \in Vor_0$$

(2) $$\forall j = 1, 2, ..., n, \quad \sum_{\xi \in S_1} \lambda_\xi \xi_j \xi_n = 0$$

(3) $$\forall j = 1, 2, ..., n, \quad \sum_{\xi \in S_1} (\lambda_\xi \xi_n) \xi_j = 0$$

(4) $$\sum_{\xi \in S_1} (\lambda_\xi \xi_n) \xi = 0 \ .$$

Quant à la condition $\langle B, X \rangle \geqslant 0 \ \forall \ \xi \in S$, elle équivaut (puisque $\xi_n \geqslant 0 \ \forall \ \xi \in S$), à

$$2a_1\xi_1 + ... + 2a_{n-1}\xi_{n-1} + a_n\xi_n \geqslant 0 \ \forall \ \xi \in S - S_0$$

c.q.f.d.

4.5 Proposition. *Soit $A_\theta = A + \theta B$ la matrice parfaite contiguë de la matrice parfaite A (supposée de norme entière m) pour le vecteur de face B. Alors θ est rationnel.*

Démonstration. :

Soit m le minimum de $A = (a_{ij})$. On a pour $\xi = \begin{pmatrix} \xi_1 \\ \vdots \\ \vdots \\ \xi_n \end{pmatrix} \in S$,

$$\sum a_{ij}\xi_i\xi_j = \langle A, \xi^t\xi \rangle = m.$$

Comme A est parfaite, ce système a une solution *unique* $A = (a_{ij})$ (en effet si A' est une autre solution, alors $\langle A - A', \xi^t\xi \rangle = 0 \ \forall \ \xi \in S$; or les $\xi^t\xi$ engendrent Vor. Donc $A - A' \in Vor^\perp = \{0\}$).

Les a_{ij} sont donc solutions d'un système de Cramer à coefficients entiers, et ils sont rationnels. Comme A_θ est parfaite et que son minimum m est entier, A_θ est rationnelle également.

D'après 4.4 les coefficients a_i de B sont solutions d'un système linéaire à coefficients entiers $\xi_1, \xi_2, ..., \xi_n$, ξ décrivant S; on peut donc les choisir entiers . θ est donc rationnel.

c.q.f.d.

4.6 Proposition. *La relation de contiguïté entre matrices $\mathfrak{R}$-parfaites est compatible avec la A_0-équivalence.*

Démonstration.

Soit A une matrice $\mathfrak{R}$-parfaite, et $A_\theta = A + \theta B$ la contiguë de A par une face B de $\mathcal{D}_A$ orthogonale à Vor_0. Soit $A' = {}^tPAP$ une matrice A_0-équivalente à A. Elle est évidemment $\mathfrak{R}$-parfaite, et l'on a :

$$ {}^tPA_\theta P = {}^tPAP + \theta\ {}^tPBP,$$

où ${}^tPBP$ est un vecteur de face de $\mathcal{D}_{A'}$, qui compte tenu des conditions (1) sur P est encore orthogonale à Vor_0. Comme ${}^tPA_\theta P$ est parfaite, c'est la contiguë de A' pour cette face.

c.q.f.d.

5. Connexité du graphe de contiguïté

Ce §5 va s'articuler autour des vecteurs de faces que nous sommes amenés à considérer. Pour certaines des démonstrations ci-dessous, on peut trouver une démonstration plus générale dans [7].

5.1 Proposition.

1)A est $\mathfrak{R}$-parfaite si et seulement si les projections orthogonales p(X) de ses vecteurs minimaux X sur $Vor_0{}^\perp$ engendrent $Vor_0{}^\perp$ (seuls interviennent en fait les vecteurs X correspondant aux $x \notin S(A_0)$,) les autres ayant une projection nulle.

2)Soit A $\mathfrak{R}$-parfaite. Notons C_A le cône convexe engendré dans $Vor_0{}^\perp$ par les demi-droites $\mathbb{R}^+p(x)$, $x \in S(A)$.

Alors les vecteurs de faces de C_A sont des vecteurs de faces du domaine de Voronoï $\mathcal{D}_A$.

Démonstration.

1)Supposons d'abord A $\mathfrak{R}$-parfaite. Comme A_0 est parfaite, d'après le théorème 2.7, A est parfaite au sens classique. Donc les X correspondant aux $x \in S(A)$ engendrent $Vor = Vor_0{}^\perp \oplus Vor_0$. Soit $M \in Vor_0{}^\perp$; $M \in Vor$, donc :

$$M = \sum_{x \in S(A)} \lambda_X X = \sum_X \lambda_X p(X) + \sum_X \lambda_X p_1(X)$$

où p_1 est la projection orthogonale sur Vor_0.

Comme $M \in Vor_0{}^\perp$, et que la somme est directe, $\sum_X \lambda_X p_1(X) = 0$. D'où :

$$M = \sum_X \lambda_X p(X).$$

Réciproquement, supposons que les p(X) engendrent$Vor_0{}^\perp$; Soit $M \in Vor$, et soit $M_1 = p(M)$ sa projection sur $M \in Vor_0{}^\perp$. Par hypothèse, il existe des coefficients $\lambda_X \in \mathbb{R}$ tels

que $M_1 = \sum_{x \notin S(A_0)} \lambda_X p(X)$. Donc $M - \sum_{x \notin S(A_0)} \lambda_X X$ appartient à Vor_0. Comme A_0 est parfaite, il existe des coefficients $\mu_X \in \mathbb{R}$ tels que $M - \sum_{x \notin S(A_0)} \lambda_X X = \sum_{x \in S(A_0)} \mu_X X$.
Les X engendrent bien Vor, et par suite A est parfaite, donc $\Re$-parfaite.

2)Le connexe C_A engendré dans ${Vor_0}^\perp$ par les demi-droites $\mathbb{R}^+ p(X)$ est la projection du domaine $\mathfrak{D}_A$ car

$$C_A = \{\sum \lambda_X p(X), \lambda_X \geqslant 0\} = p(\sum \lambda_X X, \lambda_X \geqslant 0) = p(\mathfrak{D}_A)$$

Soit B un vecteur de face de C_A dans ${Vor_0}^\perp$.

(a) Puisque B est dans ${Vor_0}^\perp$, alors son orthogonal $B^\perp$ dans Vor contient Vor_0 qui est engendré par des vecteurs mininmaux de A (car A_0 est parfaite).

(b) B étant un vecteur de face de C_A dans ${Vor_0}^\perp$, donc $B^\perp$ contient un hyperplan $\mathcal{P}$ de ${Vor_0}^\perp$ engendré par des p(X), X représentant $x \in S(A)$.

D'après (a) et (b), $B^\perp = Vor_0 \oplus \mathcal{P}$ est engendré par des vecteurs minimaux X de A. Tous les vecteurs minimaux X sont tels que $\langle B, p(X)\rangle \geqslant 0$ car B est vecteur de face de C_A. Mais $\langle B, X\rangle = \langle B, p(X)\rangle$, car $B \in {Vor_0}^\perp$. Donc pour tout X minimal, $\langle B, X\rangle \geqslant 0$. $B^\perp$ est donc une face d'appui de $\mathfrak{D}_A$.

c.q.f.d.

5.2 Corollaire.

Soit F une matrice ∈ Vor, telle que $p(F) \notin \mathfrak{D}_A$. Alors, il existe un vecteur de face $B \in {Vor_0}^\perp$ de $\mathfrak{D}_A$, tel que$\langle B, F\rangle < 0$.

Démonstration.

En effet :

$$p(F) \notin \mathfrak{D}_A \Leftrightarrow p(F) \notin C_A.$$

Il existe donc un vecteur de face B du convexe C_A donc de $\mathfrak{D}_A$ tel que $\langle p(F), B\rangle = \langle F, B\rangle$ soit négatif.

Enonçons un résultat qu'on utilisera dans la démonstration du théorème de connexité qu'on appellera ici *lemme de Voronoï.*

c.q.f.d.

5.3 Lemme (Voronoï).

Soient F une matrice définie positive, K et m deux constantes strictement positives. Alors l'ensemble des matrices parfaites A de minimum m vérifiant $\langle A, F\rangle \leqslant K$, est fini.

Voronoï, écrit à la page 134 de son article [8] a) :

«*il est aisé de démontrer que le nombre des formes φ_i parfaites ayant le minimum m et vérifiant*

$$\langle f, \varphi\rangle = \langle f, \varphi_1\rangle = ...$$

est fini », mais ne fait pas la démonstration.

Pour un bon nombre de lecteurs (dont moi même), l'aisance dont parle Voronoï n'est pas du tout certaine. Aussi, voilà une démonsration du lemme (c.f. [10]) avec l'hypothèse $\langle A, F\rangle \leqslant K$ plus générale que celle de Voronoï.

D'abord deux remarques :

Remarque 1.

Soit $M = (m_{ij})$ une matrice symétrique positive (i.e de valeurs propres $\mu_i \geqslant 0$). On a :

$$\frac{1}{n} max(\mu_i) \leqslant max\,|m_{ij}| \leqslant \|M\| \leqslant Tr(M) \leqslant n.max(\mu_i)$$

Démonstration.

*)$max(\mu_i) \leqslant \sum_{i=1}^{n} \mu_i$. Or $\sum_{i=1}^{n} \mu_i = Tr(M) = \sum_{i=1}^{n} m_{ii}$. Mais $\sum_{i=1}^{n} m_{ii} \leqslant n.max\,|m_{ij}|$.

Finalement $max(\mu_i) \leqslant n.max\,|m_{ij}|$, i.e $\frac{1}{n} max(\mu_i) \leqslant max\,|m_{ij}|$

*) On a $max\,|m_{ij}| \leqslant \sqrt{\sum_{\substack{i=1\ldots n\\ j=1\ldots n}} {m_{ij}}^2}$. Par ailleurs $\|M\|^2 = Tr(M^2) = \sum_{\substack{i=1\ldots n\\ j=1\ldots n}} {m_{ij}}^2$, et par suite :

$$max\,|m_{ij}| \leqslant \|M\|$$

*)On a

$$(\sum_{i=1}^{n} \mu_i)^2 = \sum {\mu_i}^2 + 2 \sum_{i<j} \mu_i \mu_j.$$

D'où l'inégalité $\sum {\mu_i}^2 \leqslant (\sum \mu_i)^2$, soit encore $Tr(M^2) \leqslant (TrM)^2$, d'où

$$\|M\| \leqslant Tr(M)\ (= \sum_{i=1}^{n} \mu_i) \leqslant n.max(\mu_i).$$

c.q.f.d.

Remarque 2.

Soit $M = (m_{ij})$ une matrice symétrique positive (i.e à valeurs propres $\geqslant 0$) et B une matrice symétrique définie positive (i.e à valeurs propres > 0). Alors :

$$\|M\| \leqslant n.\langle M, B\rangle.\left\|B^{-1}\right\|$$

Démonstration.

Comme toute matrice symétrique réelle est semblable à une matrice diagonale, on peut supposer B diagonale car :

Soient C, D, Q, trois matrices de Vor avec Q une matrice inversible.

On a :

$$Tr(Q^{-1}CQQ^{-1}DQ) = Tr(Q^{-1}CDQ) = Tr(DQQ^{-1}C) = Tr(DC) = Tr(CD)$$

Ce qui veut dire $\langle C, D\rangle = \langle Q^{-1}CQ, Q^{-1}DQ\rangle$: la transformation $T \mapsto Q^{-1}TQ$ conserve le produit scalaire. Soit alors

$$B = \begin{pmatrix} \lambda_1 & 0.. & 0.. \\ 0.. & \lambda_2 & ... \\ 0.. & 0.. & ..... \\ 0.. & 0.. & \lambda_n \end{pmatrix}, \text{ avec } \lambda_i > 0 \quad .$$

$\langle M, B\rangle = \sum_{i=1}^{n} \lambda_i m_{ii}$. Comme M est positive, les m_{ii}sont $\geqslant 0$.

$$\langle M, B\rangle \geqslant (\sum_{i=1}^{n} m_{ii}.(min\lambda_i) = TrM.(min\lambda_i) \geqslant \|M\| .(min\lambda_i)$$

car $TrM \geqslant \|M\|$ d'aprés la remarque 1. Or $min(\lambda_i) = \dfrac{1}{max(\frac{1}{\lambda_i})}$ et $\dfrac{1}{\lambda_i}$ est valeur propre de B^{-1}. Donc d'après la remarque 1,

$$\frac{1}{n}.max(\frac{1}{\lambda_i} \leqslant \left\|B^{-1}\right\| \ i.e \ max(\frac{1}{\lambda_i}) \leqslant n. \left\|B^{-1}\right\| .$$

D'où :

$$\langle M, B\rangle \geqslant \|M\| .(min\lambda_i) \geqslant \|M\| \frac{1}{max(\frac{1}{\lambda_i})} \geqslant \frac{\|M\|}{n. \left\|B^{-1}\right\|}$$

c.q.f.d.

Passons à la démonstration du lemme de Voronoï.
La connaissance des vecteurs minimaux d'une matrice parfaite permet de retrouver cette matrice de facon unique. Il s'agit donc de montrer que l'ensemble des matrices X représentant dans l'espace de Voronoï les vecteurs minimaux des matrices A vérifiant les conditions du lemme est fini. Il suffit pour cela de montrer que les matrices X vérifiant $\langle A, X\rangle = m$ sont bornées pour la norme $\|.\|$ (et donc notamment pour la norme sup(coefficients de la matrice)).

Or d'après la remarque 2, on a

$$\|X\| \leqslant nm \left\|A^{-1}\right\|$$

Reste donc à montrer que $\left\|A^{-1}\right\|$ est borné.

Notons $\lambda_1, \lambda_2, ..., \lambda_n$ les valeurs propres de A, et supposons $0 < \lambda_1 \leqslant \lambda_2 \leqslant ... \leqslant \lambda_n$. Alors, $\dfrac{1}{\lambda_1} \geqslant \dfrac{1}{\lambda_2} \geqslant ... \geqslant \dfrac{1}{\lambda_n}$ sont les valeurs propres de A^{-1}.

On a $\left\|A^{-1}\right\| \leqslant n.\dfrac{1}{\lambda_1}$ d'après la remarque 1. Pour minorer λ_1, nous allons utiliser la constante d'Hermite via le determinant de A :

$$\det A = \lambda_1.\lambda_2....\lambda_n \leqslant \lambda_1.(n\,\|A\|)^{n-1}$$

(car $\lambda_j \leqslant n\,\|A\|$ d'après la remarque 1) ce qui donne $\dfrac{1}{\lambda_1} \leqslant \dfrac{(n\,\|A\|)^{n-1}}{\det A}$ et par suite

$$\left\|A^{-1}\right\| \leqslant n.\frac{1}{\lambda_1} \leqslant n\frac{(n\,\|A\|)^{n-1}}{\det A}$$

Mais d'après le théorème d'Hermite $\gamma(A) = \dfrac{minA}{(\det A)^{\frac{1}{n}}} \leqslant \gamma_n$, on arrive à $\dfrac{1}{\det A} \leqslant \dfrac{{\gamma_n}^n}{m^n}$.

L'inégalité $\left\|A^{-1}\right\| \leqslant n\dfrac{(n\,\|A\|)^{n-1}}{\det A}$ entraîne $\left\|A^{-1}\right\| \leqslant \dfrac{n^n\|A\|^{n-1}.{\gamma_n}^n}{m^n}$. Or $\langle A, F\rangle \leqslant K$, ce qui implique, grâce à la remarque 1 appliquée à $M = A$ *et* $B = F$,

$$\|A\| \leqslant n.\langle A, F\rangle \left\|F^{-1}\right\| \leqslant n.K.\left\|F^{-1}\right\|$$

Donc en posant $K' = n.K.\left\|F^{-1}\right\|$, on arrive finalement à

$$\|X\| \leqslant n.m.n^n.{K'}^{n-1}.\frac{{\gamma_n}^n}{m^n},$$

majoration indépendante de A.

Comme les coefficients de X sont entiers, les matrices X possibles forment un ensemble fini, et par suite l'ensemble des matrices A est un ensemble fini.

c.q.f.d.

5.4 Proposition.

Étant données A et F définies positives dans $\mathfrak{R}$, avec A $\mathfrak{R}$-parfaite, il existe un chemin $A_0, A_1, ..., A_k$ de matrices $\mathfrak{R}$-parfaites contiguës de proche en proche (A_i contiguë à A_{i+1}) telles que $p(F) \in p(\mathfrak{D}_{A_k}) = C_{A_k}$.

Démonstration. :

* Si $p(F) \in p(\mathfrak{D}_A)$, prendre $A_k = A$

* Si $p(F) \notin p(\mathfrak{D}_A)$, alors $p(F) \notin \mathfrak{D}_A$, et par suite d'après 5.2, il existe un vecteur de face de $\mathfrak{D}_A, B_1 \in {Vor_0}^{\perp}$ tel que $\langle B_1, F\rangle < 0$. B_1 est de la forme :

$$\left(\begin{array}{ccc|c} & & & a_1 \\ & & & a_2 \\ & 0 & & \dots \\ & & & \dots \\ \hline \dots & \dots & \dots & \dots \\ a_1 & \dots & \dots & a_n \end{array}\right).$$

Soit A_1 la contiguë à travers cette face. D'après Voronoï, A_1 est de la forme :

$A_1 = A + \rho_1 B_1$ avec $\rho_1 > 0$, donc

$$A_1 = \left(\begin{array}{ccc|c} & & & *_1 \\ & A_0 & & *_2 \\ & & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ *_1 & \cdots & \cdots & *_n \end{array}\right),$$

et $m(A_1) = m(A)$. On a $\langle A_1, F\rangle = \langle A, F\rangle + \rho_1\langle B_1, F\rangle$. Comme $\langle B_1, F\rangle < 0$, on a $\langle A_1, F\rangle < \langle A, F\rangle$. Alors :
Ou bien $p(F) \in p(\mathfrak{D}_{A_1})$, et prendre $A_k = A_1$.
Ou bien $p(F) \notin p(\mathfrak{D}_{A_1})$, et alors $p(F) \notin \mathfrak{D}_{A_1}$ et d'après 5.2 il éxiste un vecteur de face de $\mathfrak{D}_{A_1}$, $B_2 \in Vor_0{}^{\perp}$ tel que $\langle B_2, F\rangle < 0$. Soit A_2 la contiguë à travers cette face. D'après Voronoï, A_2 est de la forme :

$A_2 = A_1 + \rho_2 B_2$ avec$\rho_2 > 0$.

$\langle A_2, F\rangle = \langle A_1, F\rangle + \rho_2\langle B_2, F\rangle$. Pour la même raison que précédemment, on arrive à $\langle A_2, F\rangle < \langle A_1, F\rangle$. En recommençant le même raisonnement, on obtient une suite décroissante

$$\ldots < \langle A_2, F\rangle < \langle A_1, F\rangle < \langle A, F\rangle$$

les A_i étant $\mathfrak{R}$-parfaits et ayant le même minimum m(A).

D'après le lemme de Voronoï (c.f. 5.3), après un nombre fini d'opérations l'algorithme s'arrête, et on arrive à $p(F) \in p(\mathfrak{D}_{A_k})$.

c.q.f.d.

5.5 Lemme.

Soient A et B deux matrices $\mathfrak{R}$-parfaites de même minimum.

Si $p(\mathfrak{D}_A) \cap \overset{o}{\overline{p(\mathfrak{D}_B)}} \neq \varnothing$, *alors* $A = B$

Démonstration.

Soit $U \in p(\mathfrak{D}_A) \cap \overset{o}{\overline{p(\mathfrak{D}_B)}}$. On a $U \in p(\mathfrak{D}_A)$ et $U \in \overset{o}{\overline{p(\mathfrak{D}_B)}}$. Il existe $F \in \mathfrak{D}_A$ tel que $U = p(F)$. Notons $(X_i)_{i=1,2,\ldots,s}$ et $(X'_i)_{i=1,2,\ldots,s'}$ les familles de vecteurs minimaux respectives de A et B. Il existe des $\beta_i > 0$ tels que

$$p(F) = \sum_{i=1}^{s'} \beta_i p(X'_i), \text{avec} \beta_i > 0 \text{ car } p(F) \in \overset{o}{\overline{p(\mathfrak{D}_B)}}. \text{ D'où : } \langle p(F), B\rangle = \sum_{i=1}^{s'} \beta_i \langle p(X'_i), B\rangle.$$

Mais $\langle X'_i, B\rangle = m(B) = m(A) \leqslant \langle X'_i, A\rangle \ \forall\, i$,
Donc $\langle X'_i, A - B\rangle \geqslant 0$. On décompose X'_i suivant $Vor_0{}^{\perp}$ et Vor_0.
$X'_i = p(X'_i) + p_1(X'_i)$ où p_1 est la projection dans Vor_0.

$$\begin{aligned} \langle X'_i, A - B\rangle &= \langle p(X'_i) + p_1(X'_i), A - B\rangle \\ &= \langle p(X'_i), A - B\rangle + \langle p_1(X'_i), A - B\rangle \\ &= \langle p(X'_i), A - B\rangle \end{aligned}$$

car $\langle p_1(X'_i), A-B\rangle = 0$ puisque $A-B \in Vor_0{}^{\perp}$. Par suite $\langle p(X'_i), A-B\rangle \geqslant 0$ c'est-à-dire $\langle p(X'_i), A\rangle \geqslant \langle p(X'_i), B\rangle$. D'où

$$\langle p(F), A\rangle \geqslant \langle p(F), B\rangle.$$

Partant de X_i vecteur minimal de A, et en faisant le même raisonnement, on arrive à :

$$\langle p(F), B\rangle \geqslant \langle p(F), A\rangle.$$

D'où $\langle p(F), A\rangle = \langle p(F), B\rangle$ ce qui donne $\langle p(F), A-B\rangle = 0$.

Soit $\langle \sum_{i=1}^{s'} \beta_i p(X'_i), A-B\rangle = 0$ i.e. $\sum_{i=1}^{s'} \beta_i \langle p(X'_i), A-B\rangle = 0$.

Or $\forall\, i\ \langle p(X'_i), A-B\rangle \geqslant 0$ et $\beta_i > 0$.

Donc $\forall\, i\ \langle p(X'_i), A-B\rangle = 0$.

Mais les $p(X'_i)$ engendrent $Vor_0{}^{\perp}$ (c.f. 5.1, 1). Donc A-B = 0 i.e : A = B.

c.q.f.d.

5.6 Lemme.

Soit A' une matrice $\mathfrak{R}$-parfaite. Alors :

$$F \in \overset{o}{\mathfrak{D}}_{A'} \Rightarrow F \textit{définie positive}$$

Démonstration. :

F s'écrit : $F = \sum_{i=1}^{s'} \beta_i X'_i$, $\beta_i > 0\ \forall\, i = 1, 2, ..., s'$, s' étant le nombre de couples de vecteurs minimaux de A', chaque vecteur minimal v_i ayant X'_i comme représentation dans l'espace de Voronoï.

Soit X un vecteur de l'espace de Voronoï représentant $x = (x_1, x_2, ..., x_n)$ *de* $\mathbb{R}^n$. Posons $X'_i = v_i = (x'_{i1}, x'_{i2}, ..., x'_{in})$. On a $\langle F, X\rangle = \langle \sum_{i=1}^{s'} \beta_i X'_i, X\rangle = \sum_{i=1}^{s'} \beta_i \langle X'_i, X\rangle$.

On remarque alors que $\forall\, i \in \{1, 2, ..., s'\}\ \langle X'_i, X\rangle = (\sum_{j=1}^{n} x'_{ij} x_j)^2 \geqslant 0$, et, comme $\forall\, i\ \beta_i$ est > 0, on a $\langle F, X\rangle \geqslant 0$.

D'autre part si $\langle F, X\rangle = 0$, alors $\sum_{i=1}^{s'} \beta_i \langle X'_i, X\rangle = 0 \Rightarrow \beta_i \langle X'_i, X\rangle = 0\ \forall\, i = 1, 2, ..., s'$ i.e : $\langle X'_i, X\rangle = 0\ \forall\, i = 1, 2, ..., s'$. Donc $X = 0$ car les X'_i engendrent l'espace.

c.q.f.d.

5.7 Théorème de connexité.
Soient A et A' deux matrices $\mathfrak{R}$-parfaites de même minimum.
Alors il existe un chemin $A_0 = A,\ A_1,\ A_2,\ ..., A_k = A'$ de matrices $\mathfrak{R}$-parfaites contiguës.

Démonstration. :
a)Si A = A' le problème ne se pose pas.
b)Si A' est contiguë à A, théoréme démontré.
c)Si A' non contiguë à A, A'est parfaite puisqu'elle est $\mathfrak{R}$-parfaite (c.f. 2.7). Donc l'intérieur $\overset{o}{\mathfrak{D}}_{A'}$ du domaine $\mathfrak{D}_{A'}$ est non vide. Soit $F \in \overset{o}{\mathfrak{D}}_{A'}$. D'après le lemme 5.6, F est définie positive. On sait qu'il existe un chemin $A_0 = A, A_1, ..., A_k$ de formes $\mathfrak{R}$-parfaites contiguës de proche en proche (A_i contiguë à A_{i+1}) telles que $p(F) \in p(\mathfrak{D}_{A_k})$ (c.f. 5.4).

Comme $F \in \overset{o}{\mathfrak{D}}_{A'}$, $p(F) \in \overset{o}{\overline{p(\mathfrak{D}_{A'})}}$. Par suite $p(F) \in p(\mathfrak{D}_{A_k}) \cap \overset{o}{\overline{p(\mathfrak{D}_{A'})}}$; et d'après le lemme 5.5, $A_k = A'$.
c.q.f.d.

6. Sur une question de finitude

On appelle *H-isométrie* de E, toute isométrie de E conservant globalement H. On sait que les réseaux $\mathfrak{R}$-parfaits sont en nombre fini à isométrie près, mais pour l'algorithme, nous avons besoin d'un résultat plus fort : sont-ils en nombre fini à *H-isométrie près?*

Nous allons montrer qu'il en est ainsi; adaptons nous à la demonstration de Voronoï qui utilise les bases d'Hermite. Nous allons construire pour les réseaux de $\mathfrak{R}$ une base de ce type commençant par une base du réseau parfait Λ_0. Tout d'abord nous donnons un lemme de relèvement :

6.1 Lemme.
Soit p la projection orthogonale de E sur la droite $H^\perp$ (orthogonal de H dans E).
Alors :
pour tout x' vecteur minimal du réseau $p(\Lambda)$, il existe x de Λ tel que : $p(x) = x'$ et $N(x) \leqslant N(x').\Psi_n$,
avec $\Psi_n = 1 + \dfrac{R_0^2 \gamma_n^n \det \Lambda_0}{N{\Lambda_0}^n}$
où : R_0 est le rayon de recouvrement de Λ_0, c'est-à-dire le rayon minimal des sphères centrées aux points de Λ_0 et qui recouvrent H (voir [5],b page 6), et γ_n la constante d'Hermite pour la dimension n.

Démonstration.
Soit $x' \in p(\Lambda)$ ($p(\Lambda) \subset H^\perp$), x' vecteur minimal, et soit $x_0 \in \Lambda$ ($\Lambda \subset E$) tel que $p(x_0) = x'$.
On a : $x' = x_0 + z$ avec $z \in H$. par définition de R_0, l existe donc $z_0 \in \Lambda_0$ tel que $N(z_0 - z) \leqslant R_0^2$.

Montrons que $x = x_0 + z_0$ répond à la question.
* x appartient à Λ, car x_0 et z_0 sont dans Λ.
* $p(x) = p(x_0 + z_0) = p(x_0) + p(z_0) = p(x_0) = x'$ car $z_0 \in \Lambda_0$ ($\subset H$). (c.f. annexe I, fig 1).
$N(x) = N(x') + N(x - x')$. Or $x - x' = x_0 + z_0 - x_0 - z = z_0 - z$. Donc $N(x - x') = N(z_0 - z) \leq R_0^2$. D'où $N(x) \leq N(x') + R_0^2$,

$$\frac{N(x)}{N(x')} \leq 1 + \frac{R_0^2}{N(x')} \tag{1}$$

Mais $\gamma_n = \dfrac{N(\Lambda)}{\det(\Lambda)^{\frac{1}{n}}} \leq \gamma_n$, avec d'une part $N(\Lambda) = N(\Lambda_0)$ et d'autre part $\det(\Lambda) = \det(\Lambda_0).N(x')$. Donc $\dfrac{N(\Lambda_0)}{[\det(\Lambda_0).N(x')]^{\frac{1}{n}}} \leq \gamma_n$, soit $\dfrac{N(\Lambda_0)^n}{\det(\Lambda_0).N(x')} \leq {\gamma_n}^n$, d'où $\dfrac{1}{N(x')} \leq \dfrac{1}{N(x')} \leq \dfrac{{\gamma_n}^n.\det(\Lambda_0)}{N(\Lambda_0)^n}$.
En revenant à l'expression (1), on obtient :
$\dfrac{N(x)}{N(x')} \leq 1 + \dfrac{{R^2}_0.{\gamma_n}^n.\det(\Lambda_0)}{N(\Lambda_0)^n}$, i.e :

$$N(x) \leq N(x').(1 + \frac{R_0^2.{\gamma_n}^n.\det(\Lambda_0)}{N(\Lambda_0)^n}).$$

c.q.f.d.

D'où l'existence de base à *la Hermite* pour tous les réseaux de la famille $\Re$:

6.2 Lemme.
Soit $\{e_1, e_2, ..., e_{n-1}\}$ *une base de* Λ_0.
Tout réseau $\Lambda \in \Re$ *admet une base* $\mathcal{B}_1 = \{e_1, e_2, ..., e_{n-1}, e_n\}$ *telle que :*

$$\frac{N(e_1)...N(e_{n-1}).N(e_n)}{\det \Lambda} \leq \rho_n(\Lambda_0),$$

où la constante $\rho_n(\Lambda_0) = \dfrac{N(e_1)...N(e_{n-1})}{\det \Lambda_0}.\Psi_n$ *ne dépend pas de* Λ.

Démonstration. :
Soit $\{{e'}_n\}$ une base de $p(\Lambda)$ (${e'}_n$ vecteur minimal dans $p(\Lambda)$). D'après 6.1, il éxiste e_n dans Λ tel que :

$$p(e_n) = {e'}_n \text{ et } N(e_n) \leq N({e'}_n).\Psi_n \tag{2}$$

Vérifions que $\mathfrak{B}_1 = \{e_1, e_2, ..., e_{n-1}, e_n\}$ est une base cherchée.

*$\mathfrak{B}_1$ est une base; en effet :
soit $x \in \Lambda$; $p(x) = x' = \beta_n e'_n$, $\beta_n \in \mathbb{Z}$. L'élément $y = \beta_n e_n$ de Λ a pour projection x' sur $H^\perp$. Donc $x - y \in H \cap \Lambda = \Lambda_0$:
il existe $\gamma_1, ..., \gamma_{n-1}$ dans $\mathbb{Z}$ tels que $x - y = \gamma_1 e_1 + ... + \gamma_{n-1} e_n$, d'où :

$$x = \gamma_1 e_1 + ... + \gamma_{n-1} e_{n-1} + \beta_n e_n.$$

$\mathfrak{B}_1$ engendre Λ, et a n éléments; c'est bien une base.

$$* \quad \frac{N(e_1)...N(e_{n-1}).N(e_n)}{\det \Lambda} = \frac{N(e_1)...N(e_{n-1})}{\det \Lambda_0} \cdot \frac{N(e_n)}{N(e'_n)}$$

$$(3) \qquad \leq \Psi_n \cdot \frac{N(e_1)...N(e_{n-1})}{\det \Lambda_0} \ .$$

Remarque: En choisissant une base d'Hermite du réseau Λ_0, c'est-à-dire une base telle que $\frac{N(e_1)...N(e_{n-1})}{\det \Lambda_0} \leq (\frac{4}{3})^{\frac{(n-1)(n-2)}{2}}$ on obtient $\rho_n(\Lambda_0) = (\frac{4}{3})^{\frac{(n-1)(n-2)}{2}} . \Psi_n$.
Dans la pratique, pour n=8, on a toujours pu choisir $e_1, e_2, ..., e_{n-1}$ minimaux, d'où

$$\rho_n(\Lambda_0) \leq \gamma_{n-1}^{n-1} . \Psi_n$$

En utilisant pour les réseaux de la famille $\mathfrak{R}$ une telle base d'Hermite, on obtient en termes de matrices et avec les notations du §4, le théorème suivant :

6.3 Théorème de finitude.
À A_0-équivalence près, il n'existe (en dimension n) qu'un nombre fini de matrices parfaites avec un coin A_0, de minimum donné m.

Démonstration.
Soit $\Lambda \in \mathfrak{R}$, rapporté à une base $\mathfrak{B}_1$ (c.f. 6.2) et $x = \xi_1 e_1 + ... + \xi_i e_i + ... + \xi_n e_n$, $\xi_j \in \mathbb{Z}$ un vecteur minimal de Λ.
Soit $\mathfrak{B}_0$ une base orthornormée de $\mathbb{R}^n$. On a :
$\det_{\mathfrak{B}_0}(e_1, e_2, ..., e_{i-1}, x, e_{i+1}, ..., e_n) = \xi_i . \det_{\mathfrak{B}_0}(e_1, e_2, ..., e_{i-1}, e_i, e_{i+1}, ..., e_n) = \xi_i \Delta(\Lambda)$.
D'après l'inégalité de Hadamard, on en déduit :

$$|\xi_i| \leqslant |\frac{\|e_1\| . \|e_2\| ... \|x\| . \|e_{i+1}\| ... \|e_n\|}{\Delta(\Lambda)}| \leqslant |\frac{\|e_1\| . \|e_2\| ... \|e_i\| . \|e_{i+1}\| ... \|e_n\| . \|x\|}{\Delta(\Lambda) . \|e_i\|}| \leqslant \frac{\|x\|}{\|e_i\|} . \sqrt{\rho_n(\Lambda_0)} \ .$$

Comme x est un vecteur minimal, $\frac{\|x\|}{\|e_i\|} \leqslant 1$. D'où : $|\xi_i| \leqslant \sqrt{\rho_n(\Lambda_0)}$.
L'ensemble $\mathcal{U}$ des n-uplets $(\xi_1, \xi_2, ..., \xi_n)$ de $\mathbb{Z}^n$ qui sont susceptibles d'être les composantes d'un vecteur minimal x d'un quelconque Λ de $\mathfrak{R}$ dans sa base $\mathcal{B}_1$, est donc fini. Or, Λ étant parfait, la matrice de Gram de Λ dans $\mathcal{B}_1$, notée $Gram(\Lambda, \mathcal{B}_1)$, est déterminée de façon unique par son minimum et par les n-uplets $(\xi_1, \xi_2, ..., \xi_n)$ de $\mathbb{Z}^n$ le représentant. On obtient donc un nombre fini de matrices parfaites de minimum donné : $G_1, G_2, ..., G_p$.

$Gram(\Lambda, \mathcal{B}_1) \in \{G_1, G_2, ..., G_p\}$.
Soit A une matrice parfaite de minimum m avec un coin A_0. C'est la matrice de Gram d'un réseau Λ $\Re$-parfait dans une base $\{e_1, e_2, ..., e_{n-1}, u_n\}$ u_n non nécéssairement égal à e_n. A est donc A_0-équivalente à $Gram(\Lambda, \mathcal{B}_1)$, donc à une matrice $G_i, i = 1, ..., p$.
c.q.f.d.

Chapitre III

ALGORITHMIQUE

Les calculs faits à la main pour trouver les contigus d'un réseau parfait sont extrêmement fastidieux pour peu que la dimension dépasse 6 ou 7. Grâce à l'ordinateur nous allons donner à cette partie de notre recherche un caractère algorithmique. Ainsi nous montrerons les différentes étapes qui ont conduit à la *table des réseaux parfaits à section hyperplane parfaite.*

Le langage de programmation utilisé est le C. Raison majeure : pouvoir se servir du logiciel **pari** écrit en C. C. Batut, D. Bernardi, H. Cohen et M. Olivier, les auteurs de ce logiciel, l'ont doté d'une multiprécision. Cela évite alors les "*overflow*" affichés à l'écran dans certains calculs. De plus, la calculette **gp** directement greffée à ce logiciel, possède de nombreuses applications déja prêtes à l'emploi: **rank** pour chercher le rang d'une matrice, **det** pour calculer un determinant, **lllgram** pour chercher une base de petits vecteurs d'un réseau, etc ..., pour ne citer que celles-là largement employées.

Toutefois les algorithmes élaborés dont on donnera l'ossature, seront décrits dans ce chapitre indépendamment de tout langage. L'avantage est de pouvoir les adapter au dialecte choisi.

Bien entendu, ces programmes peuvent toujours être affinés jusqu'à les rendre de plus en plus performants et nous n'avons pas la prétention de dire ici qu'ils le sont.

7. Algorithmes de base

Comment traduire à la machine les notions de réseau, perfection de réseau, spectre de reseau ... ? C'est ce lien que nous allons essentiellement résumer ici.

Un réseau Λ est défini par une matrice de Gram A=Gram($\Lambda, \mathfrak{B}$) relativement à une base $\mathfrak{B}$ de Λ. Pour la machine, un réseau est donc un tableau de nombres. Une fois ces nombres introduits, un programme approprié devrait être capable de donner les résultats dont on aura besoin, comme par exemple l'ensemble $S(\Lambda)$ des vecteurs minimaux de Λ, le déterminant det (Λ), la norme N(Λ) notée aussi m, la constante d'Hermite $\gamma(\Lambda)$, la perfection, le spectre spect(Λ) (qu'on définira au §7.4).

Nous allons décrire la plupart des fonctions qui nous intéressent, à part certaines figurant déjà dans la bibliothèque **gp**, ou trop classiques pour être étudiées. Nous en donnerons le

plan de l'algorithme sans rentrer dans les détails pour ne pas perdre le fil conducteur.

7.1 Symboles.

Adoptons une façon d'écrire un programme. Pour cela on va s'inspirer des livres de H. Cohen (A course in algorithmic algebraic number theory) et de A. Engel (Mathématique élémentaire d'un point de vue algorithmique).

Les instructions élémentaires pour décrire un algorithme seront écrites avec des symboles que nous allons définir. Rappelons que la *mémoire* d'un ordinateur est constituée de *régistres* ou *variables*, qu'on imaginera comme des cases dotées d'adresses, et dans lesquelles on peut écrire un nombre. On les désignera par une lettre alphabétique ou un mot.

a)Pour affecter une valeur donnée à une variable, on écrira $\longleftarrow$; par exemple $A \longleftarrow 4$: mettre 4 dans la variable A.

(Si la variable A est déjà occupée par une valeur, elle sera remplacée par 4).

b)$X \longleftarrow f(A,B)$: calculer d'abord f(A,B), et mettre le résultat dans la variable X.

c)$X \longleftrightarrow Y$: les variables X et Y vont s'échanger leurs valeurs respectives.

d)Fichier1 $\longleftarrow$ fichier2: le contenu de fichier2 va s'inscrire dans fichier1.

e)Écrire(A,B,'expression') : écrire les valeurs de A,B et l'expression.

f)Introduire (A, B) : introduire les valeurs de A et de B.

g)Si (instruction1) alors (instruction2) sinon (instuction3) : test de décision.

h){instruction1; instruction2;...} : bloc d'instructions.

i)Fin : le programme s'arrête.

j)Le point virgule (;) sépare les instructions.

k)Les commentaires se font à l'intérieur des crochets.

l)Les lignes sont numérotées dans l'ordre d'exécution de l'algorithme. Si plusieurs instructions sont écrites dans une ligne, l'exécution de l'une d'elles est subordonnée à l'exécution de la précédente, sinon on passe à la ligne suivante.

7.2 Invariants d'un réseau. .

L'un des premiers programmes écrits est le programme **vm**. Il donne essentiellement à partir de la matrice de Gram A d'un réseau Λ, l'ensemble $S(\Lambda)$, et par dénombrement le cardinal s. Les autres invariants de Λ (*ie* : $\gamma(\Lambda)$, $\det(\Lambda)$, $N(\Lambda)$) s'en suivent formellement(c.f 0.1). C'est un programme banal, retrouvé un peu partout dans la littérature sur les réseaux; il se base sur la réduction de Gauss d'une forme quadratique (décomposition en carrés). La calculette **gp** possède également une fonction analogue, la fonction **minim** de C. Batut.

7.3 Test de perfection de réseau. .

Soit Λ un réseau de E de dimension n, $\mathfrak{B} = \{e_1, e_2, ..., e_n\}$ une de ses bases, A=Gram($\Lambda, \mathfrak{B}$) et $S(\Lambda)$ l'ensemble des vecteurs minimaux (distincts au signe près). Nous allons énoncer

un critère de perfection plus pratique que la propostion 3.4; en fait c'est une autre interprétation qui lui est équivalente. Pour cela on identifie l'espace de Voronoï de dimension $N = \frac{n(n+1)}{2}$ à $\mathbb{R}^N$, et on considère l'application :

$$t : S(\Lambda) \longrightarrow \mathbb{R}^N$$

définie pour $x_h = (k_{1h}, ..., k_{nh})$ dans $S(\Lambda)$ par

$$t(x_h) = ({k^2}_{1h}, k_{1h}k_{2h}, ..., {k_{nh}}^2).$$

7.3.1 Propostion. *Pour que Λ soit parfait il faut et il suffit que t(S) soit de rang N.*

Démonstration. Pour tout $h = 1, 2, ..., s$, on a : $x_h = \sum_{i=n}^{n} k_{ih}e_i$, $k_{ih} \in \mathbb{Z}$.

Si $m = N(\Lambda)$, alors $N(x_h) = m \ \forall \ h = 1, 2, ..., s$.

Ce qui s'écrit encore :

$\sum_{1 \leq i,j \leq n} k_{ih}k_{jh}e_i.e_j = m \ \forall \ h = 1, 2, ..., s$.

En posant $a_{ij} = e_i.e_j$, et en tenant compte de ce que $a_{ij} = a_{ji}$, on a un système de s équations à N inconnues, de la forme :

$$\sum_{1 \leq i,j \leq n} k_{ih}k_{jh}a_{ij} = m \ \forall \ h = 1, 2, ..., s.$$

La condition nécessaire et suffisante s'ensuit :

Λ parfait veut dire que les coefficients a_{ij} sont complètement déterminés à partir de ce système (c.f. ii de o.6); donc le rang de la matrice $(k_{ih}k_{jh})$ est égal à N (système de Cramer). Ce qui signifie que t(S) est de rang N.

D'où l'idée de chercher le rang de t(S) pour tester la perfection. L'application **rank** de la calculette **gp** est ici la bienvenue, comme le programme élémentaire **rang** élaboré en ce sens.

7.3.2 Algorithme perf.

1)Introduire les coefficients a_{ij} de A=Gram($\Lambda, \mathfrak{B}$).

2)[Initialisation]$j \longleftarrow 1$; $h \longleftarrow 1$.

3)[Application **vm***] Trouver un vecteur minimal distinct (au signe près) de ceux déjà trouvés: $x_h = (k_{1h}, ..., k_{nh})$.*

4)[Fin?] Si (pas de nouveau vecteur minimal) alors {écrire ('réseau non parfait'); fin.}

5)[Calcul de $t(x_h)$] $t(x_h) = ({k^2}_{1h}, k_{1h}k_{2h}, ..., {k_{nh}}^2)$.

6)[v_j est un vecteur à N composantes] $v_j \longleftarrow t(x_h)$.

7)[Application **rang***] Calculer le rang de $\{v_1, v_2, ..., v_j\}$.*

8)[Fin?] Si (rang = N) alors {écrire ('réseau parfait'); fin.}

9)Si (rang = j) alors ($j \longleftarrow j + 1$).

10)$h \longleftarrow h+1$*; aller ligne 3.*

Commentaires.
La ligne 8 indique qu'il est superflu de continuer à chercher les autres vecteurs minimaux dès lors que le rang est N. En effet, chaque vecteur qui va suivre est combinaison linéaire des précédents.

7.4 Spectre d'un réseau.

Nous allons définir un autre invariant du réseau Λ de norme m : le spectre qu'on notera spect(Λ).

7.4.1 Propostion. *Pour tous v,x dans* $S(\Lambda)$, $x \neq v$, *on a :*

$$|v.x| \leq \left\lfloor \frac{m}{2} \right\rfloor$$

Démonstration. On a les implications suivantes :

$$N(x+v) \geq m$$

$$\Rightarrow N(x)+N(v)+2(v.x) \geq m$$

$$\Rightarrow 2m+2(v.x) \geq m$$

$$\Rightarrow v.x \geq -\tfrac{m}{2}.$$

De même, $N(x-v) \geq m$ implique $v.x \leq \dfrac{m}{2}$.
Donc

$$|v.x| \leq \left\lfloor \frac{m}{2} \right\rfloor.$$

c.q.f.d.

D'après la proposition précédente, les éléments de cet ensemble sont parmi les entiers 0,1,2,..., $\left\lfloor \dfrac{m}{2} \right\rfloor$.

Notons n_i le nombre de couples $\pm x$ tels que $x.v = i$, i variant de 0 à $\left\lfloor \dfrac{m}{2} \right\rfloor$.

7.4.2 Définition. *a)Le* **spectre de v** *est la suite ordonnée* $(n_0, n_1, ..., n_{\lfloor \frac{m}{2} \rfloor})$.
b)Le **spectre d'un réseau** *est la liste des spectres des vecteurs minimaux avec le nombre de fois qu'on les obtient.*

L'intérêt d'étudier le spectre d'un réseau Λ repose sur la remarque suivante:

7.4.3 Remarque. *Si σ est une isométrie de Λ sur Λ', alors:*

$$\forall\, v \in S(\Lambda),\ spect(v) = spect(\sigma v)$$

En effet $\forall\, x \in S(\Lambda)$, $\sigma x.\sigma v = x.v$. Quand x décrit S(Λ), σx décrit $S(\Lambda)$ qui est égal à $S(\Lambda')$.

$$\text{Donc } spect(v) = spect(\sigma v)$$

Ceci entraîne que deux réseaux isométriques ont le même spectre. On pourra alors utiliser la contraposée comme test:

si Λ et Λ' n'ont pas le même spectre, ils ne sont pas isométriques.

Voici donc:

7.4.4 Algorithme spect.

1) Introduire les coefficients de la matrice de Gram A du réseau Λ.

2) [Application **vm***] Chercher $S(\Lambda)$, s, et la norme m de Λ.*

3)[Initialisation] $j \longleftarrow 0$.

4)Prendre v dans S s'il n'a pas déjà été choisi.

5)[Boucle] Pour tous les x de S, $x \neq \pm v$, calculer $|v.x|$ $(= |{}^t vAx|)$.

6)[Boucle] De i=0 à $\left\lfloor \frac{m}{2} \right\rfloor$, dénombrer les couples $\pm x$ pour lesquels $|x.v| = i$: il y en a n_i.

7)[Spect(v)] Stocker $(n_0, n_1, ..., n_{\lfloor \frac{m}{2} \rfloor})$ dans un tableau T; $j \longleftarrow j + 1$; si $(j \neq s)$ aller ligne 3.

8)[Spect(Λ)] Dénombrer le nombre de fois qu'on trouve le même spectre de vecteur dans le tableau T; fin.

Commentaires.

À la ligne 4, il faut prendre les vecteurs dans S(Λ) l'un après l'autre. Cela suppose qu'ils ont été mémorisés et numérotés.

8. Algorithmes d'isométrie

On sait qu'un même réseau peut être représenté par une infinité de matrices de Gram. Mais alors deux matrices de Gram A et A' étant données, comment savoir si elles représentent le même réseau? L'idée est de trouver une matrice P de $Gl_n(\mathbb{Z})$ telle que $A' = {}^t PAP$. Le programme **isom** de C. Batut via D.O. Jaquet apporte la réponse dans le cas où A est écrite dans une base de vecteurs minimaux.

Voilà pourquoi il est intéressant de chercher d'abord une base de vecteurs minimaux si elle existe.

8.1 Base de vecteurs minimaux.

L'application **lllgram** de la calculette **gp** donne pour un réseau Λ de matrice de Gram A, une base formée de petits vecteurs. Ces petits vecteurs sont pour la plupart des vecteurs minimaux du réseau, mais il n'en est pas toujours ainsi. Aussi devons-nous construire un programme adapté exactement à notre problème. Autrement dit on impose à A d'avoir un coin A_0, où A_0 est écrite dans une base de vecteurs minimaux (ce qui est toujours possible pour $n \leq 7$).

Nous avons alors le résultat suivant :

8.1.1 Proposition.

Soit $\mathfrak{B}_1 = \{e_1, e_2, ..., e_n\}$ une base de Λ telle que $e_1, e_2, ..., e_{n-1}\}$ soit une base de vecteurs minimaux de Λ_0, et soit $\mathfrak{B}_2 = \{e_1, e_2, ..., e_{n-1}, x\}$ un ensemble de vecteurs minimaux de Λ avec $x = a_1e_1 + a_2e_2 + ... + a_ne_n$.

Pour que $\mathfrak{B}_2$ soit une base de Λ il faut et il suffit que $|a_n| = 1$.

Démonstration. Supposons $\mathfrak{B}_2 = \{e_1, e_2, ..., e_{n-1}, x\}$ base de Λ. La matrice de passage de $\mathfrak{B}_2$ à $\mathfrak{B}_1$ est:

$$P = \begin{pmatrix} 1 & 0 & .. & 0 & a_1 \\ 0 & 1 & .. & 0 & a_2 \\ .. & 0 & .. & .. & ... \\ .. & .. & .. & .. & ... \\ 0 & 0 & .. & 1 & a_{n-1} \\ 0 & 0 & ... & 0 & a_n \end{pmatrix}$$

Comme $P \in Gl_n(\mathbb{Z})$, on a $\det(P) = \pm 1$, *ie* $|a_n| = 1$

Réciproquement : supposons $|a_n| = 1$.

$\mathfrak{B}_2$ est formée de vecteurs linéairement indépendants. Considérons le réseau Λ' engendré par $\mathfrak{B}_2$ dans Λ. L'indice $[\Lambda : \Lambda']$ est égal à $|\det_{\mathfrak{B}_1} \mathfrak{B}_2|$.

On trouve $[\Lambda : \Lambda'] = |a_n| = 1$.

D'où $\Lambda' = \Lambda$, et par suite $\mathfrak{B}_2$ est une base de Λ.

c.q.f.d.

On a donc une méthode pour chercher une base de vecteurs minimaux :

À partir de la proposition précédente, on voit qu'il faut d'abord chercher $S(\Lambda)$, puis de repérer le premier vecteur minimal x dont la dernière composante est ± 1.

Ce qui donne l'algorithme suivant:

8.1.2 Algorithme nvgram.

1)Introduire les coefficients de $A = Gram(\Lambda, \mathfrak{B}_1)$.

2)[Application **vm***] Trouver un vecteur minimal $v = (a_1, a_2, ..., a_n)$ distinct (au signe près) de ceux déjà trouvés.*

3)[Fin?] Si (pas de nouveau veceur minimal) écrire ('pas de base de vecteurs minimaux');fin.

4)[Test du choix d'un vecteur minimal x] Si ($|a_n| = 1$) alors ($x \longleftarrow v$) sinon (aller à ligne 2).

5)[Calcul de produits scalaires] Chercher $B = Gram(\Lambda, \{e_1, e_2, ..., e_{n-1}, x\})$.

6)Ecrire('nouvelle matrice de Gram : ' B);fin.

Commentaires.

La ligne 4 indique qu'il n'est pas besoin de continuer à chercher $S(\Lambda)$ en entier. En effet, si le vecteur x est repéré, on passe tout de suite au calcul de la nouvelle matrice de Gram B. C'est notre but.

8.2 Isométrie de réseaux.

Il est clair que si deux réseaux Λ et Λ' se différencient par au moins un de leurs invariants alors ils sont distincts.

Et s'ils ont les mêmes invariants sont-ils pour autant isométriques?

Le problème est d'essayer de construire une isométrie $f : \Lambda \longrightarrow \Lambda'$ sachant que Λ possède une base de vecteurs minimaux $\mathfrak{B} = \{e_1, e_2, ..., e_n\}$.

Si une telle f existe on a les remarques suivantes:

8.2.1 Remarques.

Pour tout i = 1, 2, ..., n :

a)e_i *et* $f(e_i)$ ont le même spectre.

b)e_i *et* $-e_i$ ont le même spectre.

c)$f(e_i)$ est un vecteur minimal de Λ.

d)$\forall\ i,\ j = 1,\ 2, ..., n, \quad f(e_i).f(e_j) = e_i.e_j,$

(ce qui entraîne que $Gram(\Lambda, \mathfrak{B}) = Gram(f(\Lambda), f(\mathfrak{B}))$)

8.2.2 Proposition.

Si $f : \Lambda \longrightarrow \Lambda'$ *est une application linéaire vérifiant la condition d, et si* $\det(\Lambda) = \det(\Lambda')$ *alors:*

a)$\{f(e_1), f(e_2), ..., f(e_n)\}$ *est une base de* $f(\Lambda)$.

b)$f(\Lambda) = \Lambda'$.

(ie f est une isométrie).

Démonstration.

a) En effet, f est injective : par linéarité on déduit de d) que $\forall x, y \in E\ f(x).f(y) = x.y$. Donc si $f(x) = 0$, on a $\forall y \in E,\ x.y = 0$. Donc $x = 0$. De cette remarque, $\lambda_1 f(e_1) + \lambda_2 f(e_2) + ... + \lambda_n f(e_n) = 0$ implique:

$$f(\lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n) = 0 \quad .$$

Comme f est injective, $\lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n = 0$.

Ce qui donne $\lambda_i = 0\ \forall\ i = 1, 2, ..., n$.

b)$f(\Lambda) \subset \Lambda'$. Comme $\det(\Lambda') = \det(\Lambda) = \det(f(\Lambda))$, on a $[\Lambda' : f(\Lambda)] = 1$. D'où $f(\Lambda) = \Lambda'$.

c.q.f.d.

Cette proposition et la remarque c nous montrent qu'un choix judicieux parmi les 2s vecteurs minimaux de Λ' des $f(e_i)$ pour i=1, 2, ..., n , vérifiant $f(e_i).f(e_j) = e_i.e_j$, constitue une solution f possible. Ce choix est ramené à un nombre fini de vérifications, qu'on peut nettement diminuer en tenant compte de la remarque a. De façon imagée le procédé de construction de f revient à prendre un grand échiquier rectangulaire n x 2s, et à placer sur chaque colonne i une reine $r_{l(i)}$ (l(i) étant le numéro de ligne) de telle manière qu'une fois posée , il n'y a pas "échec" aux conditions (I) suivantes:

8.2.3 Conditions (I).

- $r_{l(i)}$ *est un vecteur minimal de* Λ'; $l(i)$ *est donc le numéro de ce vecteur.*
- $r_{l(1)}$, $r_{l(2)}$, ..., $r_{l(i)}$ *sont distincts (ie f est une injection).*
- $r_{l(i)}.r_{l(j)} = e_i.e_j$ *pour tout j = 1, 2, ..., i-1.*
- $spect(r_{l(i)}) = spect(e_i)$.

Dans ce cas nous conviendrons de dire que *l(i) convient*, ce qui sous entend que la case de colonne i et de ligne l(i) convient pour poser la reine, ou encore que les conditions (I) sont satisfaites, c'est à dire le vecteur de Λ' de numéro l(i) convient pour être l'image de e_i par f.

C'est le problème bien connu des " n reines sur un échiquier", qui utilise la technique classique du *back-tracking* pour trouver une solution, et qui se résume ainsi:

Dans la 1^e colonne on pose la 1^e reine sur la case l(1)=1. Dans la 2^e colonne on essaye successivement les cases de bas en haut pour en trouver une qui convienne à la 2^e reine. On fait de même dans la 3^e colonne pour la 3^e reine. Et ainsi de suite. Si dans la colonne n^0 i aucune des 2s cases ne convient à la reine n^0 i, on revient à la colonne précédente n^0 i-1 et on cherche une autre case qui convienne à la reine n^0 i-1; etc....

L'ordinateur donnera l'isométrie f sous forme d'un n-uplet f = (l(1), l(2),..., l(n)).

On arrive donc au programme que voici:

8.2.4 Algorithme gisom.

1)Introduire A (obligatoirement écrite dans une base de vecteurs minimaux), et A'.

2)[Application **vm***] Chercher les invariants s(A),s(A'),det (A),det (A'), N(A) et N(A').*

3)[Test] Si (l'un des invariants diffère) alors {écrire ('réseaux non isométriques: invariants différents);fin}.

4)[Calcul de produits scalaires] Recueillir les produits scalaires 2 à 2 des 2s vecteurs minimaux de Λ'; recueillir les produits scalaires 2 à 2 des éléments de $\mathfrak{B} = \{e_1, e_2, ..., e_n\}$, base canonique de Λ).

5)[Application **spect***] Recueillir les spectres des 2s vecteurs minimaux de Λ'; recueillir les spectres des éléments de $\mathfrak{B} = \{e_1, e_2, ..., e_n\}$.*

6)[Initialisation] i $\longleftarrow$ 1.

7)[Initialisation] l(i) ⟵ 1.
8)[Test] Si (l(i) ne convient pas) aller ligne 10.
9)[Fin?] i ⟵ i+1; Si (i > n) alors {écrire(l(1),l(2),...,l(n)); fin } sinon (aller ligne 7).
10)[Incrémentation] l(i) ⟵ l(i)+1.
11)[Test] Si ($l(i) \leq 2s$) aller ligne 8.
12)[Back-tracking] $i \longleftarrow i-1$.
13)[Test] Si ($i \neq 0$) aller ligne 10.
14)[Fin] Écrire ('Aucune isométrie malgré les mêmes invariants') ; fin.

Commentaires.
1)La matrice P de $Gl_n(\mathbb{Z})$ telle que ${}^tPAP = A'$ est connue dès lors que l'isométrie f=(l(1),...,l(n)) est trouvée. C'est la matrice des vecteurs colonne $r_{l(i)}$ pris dans $S(\Lambda')$.

De la ligne 1 à la ligne 5, la machine calcule surtout des résultats qu'elle stocke dans des tableaux. Les instructions clefs se jouent véritablement de la ligne 6 à la ligne 14; elles forment un processus étonnant par le peu d'étapes, et important par le rôle qu'il a joué en tant que filtre de réseaux.

2)L'algorithme que nous avons présenté a été mis en place en s'inspirant des notes prises lors de la visite de Jaquet à Bordeaux, et de certaines remarques instructives de C. Batut dont on a utilisé le programme **isom**.

Par contre pour des vérifications, on s'est surtout servi de **gisom**.

8.2.5 Variantes du programme gisom.

1)On peut enlever l'instruction *fin* à la ligne 9 et mettre à la place un compteur et l'instruction $i \longleftarrow i-1$; c'est le programme **ngisom** qui donne le nombre g d'isométries.

Si A=A', g sera alors le nombre d'automorphismes (qui est un autre invariant de réseau).

2)L'étude faite au § 1 nous amène à comparer deux matrices A et A' à coin A_0. Il faut donc s'intéresser à une isométrie f qui conserve Λ_0 (ie $f(\Lambda_0) = \Lambda_0$), qu'on appellera *H-isométrie*, H étant l'hyperplan de E engendré par Λ_0. À supposer que $\{e_1, e_2, ..., e_{n-1}\}$ est base de Λ_0, cela revient à rajouter aux conditions (I) la condition supplémentaire:

$$f(e_i) \in \{e_1, e_2, ..., e_{n-1}\} \ \forall\ i = 1,\ 2, ...,\ n-1.$$

Ceci impose la dernière composante de $f(e_i)$ nulle. Les conditions (I) deviennent alors les conditions (I'):

- $r_{l(i)}$ est un vecteur minimal de Λ'; l(i) est donc le numéro de ce vecteur.
- $r_{l(1)}$, $r_{l(2)}, ...,$ $r_{l(i)}$ sont distincts (ie f est une injection).
- $r_{l(i)}.r_{l(j)} = e_i.e_j$ pour tout j = 1, 2, ..., i-1.
- $spect(r_{l(i)}) = spect(e_i)$.
- la n^e composante de $r_{l(i)}$ est nulle.

... et nous avons le programme **hisom**, *celui qu'on utilisera véritablement dans le programme final pour chercher les contigus.*

3)Dans les mêmes considérations que le 1) on peut chercher le nombre h de H-isométries; c'est le programme **nhisom**.

9. Algorithme de contiguïté

Soit Λ un réseau parfait de matrice de Gram A, au-dessus de Λ_0 parfait de matrice de Gram A_0.

Quels sont les contigus de Λ ayant pour section hyperplane Λ_0? Comment les chercher? Nous allons tâcher d'y répondre en construisant un programme qui jouera un rôle de 1er plan dans ce travail.

9.1 Initialisation de l'algorithme de Voronoï.

Du fait de la connexité du graphe de contiguïté (c.f. §5), l'existence d'un seul réseau parfait Λ au dessus de Λ_0, suffit pour trouver tous les autres par l'algorithme de Voronoï. Le problème est de savoir si effectivement il y en a un. On peut s'intéresser par exemple aux réseaux entiers, ce sont les plus simples. Dans le cas n=8 que nous traitons, la propostion suivante nous donne une réponse encore plus précise:

9.1.2 Proposition.

Soit Λ_0 un réseau parfait en dimension 7, de matrice de Gram A_0:

1) Λ_0 admet une base $\mathfrak{B}_0$ de vecteurs minimaux.

2)Il existe un réseau parfait Λ, de base $\mathfrak{B}$, au-dessus de $\Lambda_0 \neq P(7,2)$,avec $\mathfrak{B}$ base de vecteurs minimaux.

3)Il n'existe pas de réseau entier parfait ayant P(7,2) comme section hyperplane, à moins de normaliser à 6.

Démonstration.

1)La table de Conway-Sloane (c.f. [5]a) donne les matrices des 33 réseaux parfaits. Il suffit d'essayer le programme **lllgram** de la calculette **gp** ou encore le programme **nvgram** sur les matrices A_0 qui n'ont pas leurs éléments diagonaux égaux au minimum. L'exécution a toujours donné une matrice équivalente à éléments diagonaux égaux.

On pourra donc toujours supposer que A_0 est donnée dans une base de vecteurs minimaux.

2)Il suffit de les chercher informatiquement et de les exhiber. Notons $A = Gram(\Lambda, \mathfrak{B})$. On sait que A admet un coin A_0, ie A est de la forme :

$$A == \left(\begin{array}{ccc|c} & & & a_1 \\ & & & a_2 \\ & A_0 & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & a_{n-1} \\ a_1 & \cdots & \cdots & a_n \end{array}\right)$$

On impose $a_n = m(= N(\Lambda_0)$. D'après la proposition 7.4.1 il suffit de faire un balayage

de chacun des a_i en valeurs entieres de $\left\lceil -\frac{m}{2} \right\rceil$ à $\left\lfloor \frac{m}{2} \right\rfloor$. On teste la perfection (application **perf**) de chaque matrice A obtenue, et on arrête le programme dès qu'on en obtient une. Cet algorithme très élémentaire construit avec n-1 boucles (et qu'on a appelé **depf**) a confirmé le résultat énoncé.

3)Par traitement informatique comme précédemment.

9.2 Recherche d'une face hyperplane de $\mathfrak{D}_A$.

Dans la théorie concernant l'algorithme de Voronoï, on se place dans l'espace Vor de dimension $N = \frac{n(n+1)}{2}$. D'après le §4, le fait d'imposer une section hyperplane Λ_0 de Λ, l'algorithme est ramené dans un sous-espace de Voronoï de dimension n. Ce qui simplifie grandement les calculs pour chercher les faces hyperplanes de $\mathfrak{D}_A$, symbolisées par le vecteur de face

$$B = \left(\begin{array}{ccc|c} & & & a_1 \\ & & & a_2 \\ & 0 & & \cdots \\ & & & \cdots \\ \hline --- & --- & --- & \cdots \\ a_1 & \cdots & \cdots & a_n \end{array} \right) \in Vor_0{}^{\perp}$$

Le corollaire 2.9 et la proposition 4.4 indiquent que l'ensemble des vecteurs minimaux de A qui engendrent l'hyperplan H_B de $\mathbb{R}^n$, est une partie C de $S - S_0$ de rang n-1.

Soit $v = (\xi_1, \xi_2, ..., \xi_n)$ un élément de H_B.

Si $C = \{v_1, v_2, ..., v_{n-1}\}$ avec $v_i = (\xi_{ij}) j = 1, 2, ...n$

l'équation

$$f(\xi_1, \xi_2, ..., \xi_n) = 2a_1\xi_1 + ... + 2a_{n-1}\xi_{n-1} + a_n\xi_n = 0 \text{ de } H_B,$$

se calcule en résolvant le système de n-1 équations à n inconnues $2a_1, 2a_2, ..., 2a_{n-1}, a_n$:

$$(I) \qquad \left\{ \begin{array}{lll} 2a_1\xi_{11} & +...+ & 2a_{n-1}\xi_{1,n-1} + a_n\xi_{1n} \quad = 0 \\ .... & ... & ..... \quad = 0 \\ 2a_1\xi_{n-1,1} & +...+ & 2a_{n-1}\xi_{n-1,n-1} + a_n\xi_{n-1,n} \quad = 0. \end{array} \right.$$

On sait qu'une inconnue peut être choisie comme paramètre de telle sorte que la matrice des coefficients des inconnues restantes soit de rang n-1.

On fixera à 1 la valeur de ce paramètre ; les autres inconnues seront alors complètement déterminées. Pour choisir l'inconnue qui sera prise comme paramètre, on cherchera tous les mineurs d'ordre n-1 extraits du système jusqu'à obtenir une valeur non nulle.

Reste à vérifier que H_B est une face de $\mathfrak{D}_A$. Les vecteurs de $S - S_0$ doivent être tous soit d'un côté soit de l'autre de H_B. Ce qui veut dire $f(x) \geq 0 \ \forall \ x = (\xi_1, ..., \xi_n) \in S - S_0$ (ou bien $f(x) \leq 0 \ \forall \ x \in S - S_0$.)

Une fois la face confirmée, il ne reste plus qu'à déduire $a_1, ..., a_n$ pour avoir B. Pour rappeler qu'une telle face est issue de C, nous conviendrons d'appeler B une *C-face.*

Il est clair que deux parties C et C' peuvent définir la même face.

9.3 Recherche de θ_0.

D'après Voronoï, il existe $\theta_0 = \frac{a_0}{b_0}$ dans $\mathbb{Q}$ tel que $A_{\theta_0} = A + \frac{a_0}{b_0}B$ soit contigu de A.

Au vu du paragraphe 4:

•) Pour $0 < \theta < \theta_0$ alors $N(A_\theta) = m$ *et* $s(A + \theta B) = \sigma$ (σ étant le nombre de vecteurs minimaux de A dans l'hyperplan H).

•) Pour $\theta = \theta_0$, alors $N(A_\theta) = m$ *et* $s(A + \theta B) > \sigma$

•) Pour $\theta > \theta_0$, alors $N(A_\theta) < m$

Pour chaque valeur rationnelle de θ testée, on calcule donc $N(A_\theta)$ *et* $s(A_\theta)$ qui permettent de situer θ par rapport à θ_0.

Pour b=1, on essaye les rationnels $\frac{a}{b}$, a parcourant $\mathbb{N}$, jusqu'à trouver θ_0 (auquel cas l'algorithme est fini), ou bien on dépasse θ_0 et alors b se change en b+1, et on refait la même opération, a décrivant $\mathbb{N}$ à partir de a=1.

L'existence de θ_0 assure que cet algorithme s'arrête après un nombre fini d'opérations.

De manière plus précise, la norme du réseau Λ correspondant à la matrice de Gram $A + \theta B$, qu'on notera $m(A + \theta B)$ suit le graphe de l'annexe I (figure2) quand θ décrit $\mathbb{R}$.

Remarques: dès que $b \geqslant 2$, on peut limiter le nombre de valeurs de $\frac{a}{b}$ à essayer; en effet soit $\frac{a_1}{b-1}$ la première valeur de $\theta = \frac{a}{b-1} - \theta_0$.

On a $\frac{a_1 - 1}{b-1} < \theta_0 < \frac{a_1}{b-1}$

Les rationnels $\frac{a}{b}$ à tester vérifient $\frac{a_1 - 1}{b-1} < \frac{a}{b} < \frac{a_1}{b-1}$ ce qui équivaut à:

$\frac{(a_1 - 1)b}{b-1} < a < \frac{ba_1}{b-1}$ ce qui en fait ne donne qu'une valeur possible pour $a \in \mathbb{N}$,

$$a = \left\lceil \frac{(a_1 - 1)b}{b-1} \right\rceil .$$

Mais dans la pratique (n=8), l'expérience a montré que les essais à faire sont très peu nombreux (valeurs trouvées: $\theta_0 = 1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}$).

La même remarque a rendu inutile (dans les cas que nous avons traités) la majoration de θ_0 par la plus petite valeur $\theta_1 > 0$ telle que $\det(A + \theta_1 B) = 0$, ainsi que l'utilisation des suites de Farey.

9.4 La recherche des contigus.

On est maintenant en mesure de donner l'ossature du programme répondant à notre question:

comment rechercher par contiguïté les réseaux parfaits Λ *ayant une section hyperplane parfaite* Λ_0?

Le théorème 6.3 assure la finitude à A_0-équivalence près de ces réseaux pour une dimension n donnée.

Nous avons alors:

9.4.1 Algorithme ctg.

[1^{e}partie]

1)Introduire la matrice parfaite A_0 du réseau parfait Λ_0 (de dimension n-1 et de norme m).

2)Si(A_0 non donnée suivant une base de vecteurs minimaux) appliquer **nvgram** *pour trouver une nouvelle matrice A_0.*

*3)[**depf**] Appliquer* **depf** *pour trouver Λ parfait symbolisé par $A = Gram(\Lambda, \mathfrak{B})$ avec un coin A_0.*

4)[Test] Si (A n'existe pas) alors (renormaliser A_0); aller ligne 3.

[2^e partie]

*5)[**vm**] Trouver $S(\Lambda)$*

6)Repérer $S_0 = S(\Lambda_0) \subset S(\Lambda_0)$. [Les n^e composantes de ces vecteurs sont nulles]

7)Prendre (une partie C à n-1 éléments non déjà choisie dans $S - S_0$) sinon (fin).

8)[C engendre-t-il un hyperplan H_B dans E? : application **rank***]*

Vérifier que rang(C)=n-1 sinon (aller ligne 7).

9)[Equation de l'hyperplan H_B] Résoudre le système (I) (c.f. 9.2).

Soit $f(x) = 2a_1\xi_1 + ... + 2a_{n-1}\xi_{n-1} + a_n\xi_n = 0$ l' équation de H_B dans E.

10)[boucle] Calculer f(x) pour tous les x de $S - S_0$ et dénombrer les x pour lesquels : f(x)=0 (on trouve z_r), $f(x) \leq 0$ (on trouve m_s), $f(x) \geq 0$ (on trouve p_s).

11)[H_B est-il une face de $\mathfrak{D}_A$?] Si ($m_s.p_s = 0$) alors (calculer B) sinon (aller ligne 7).

12)[Cardinal de l'ensemble des x de S tels que f(x)=0] $\sigma \longleftarrow s(\Lambda_0) + z_r$.

[3^e partie]

13)[Initialisation] $b \longleftarrow 1; a \longleftarrow 1$.

14)$\theta \longleftarrow \frac{a}{b}; A_\theta \longleftarrow A + \theta B$.

15)[application **vm***] Chercher $s(A_\theta), N(A_\theta)$.*

16)[Test] Si $\{N(A_\theta) = m; s(A_\theta) = \sigma\}$ alors $\{a \longleftarrow a + 1$; aller ligne 14.$\}$

17)[Test] Si $(N(A_\theta) \leq m)$ alors $\{b \longleftarrow b + 1; a \longleftarrow 1$; aller ligne14$\}$.

18)[Test] Si $\{N(A_\theta) = m; s(A_\theta) \geq \sigma\}$ alors $\{\theta_0 = \frac{a}{b}$; appliquer **vm** *à $A_{\theta_0}\}$; recueillir dans le fichier* **resparf8** *: les coefficients de la dernière colonne de A_{θ_0}, $s(A_{\theta_0})$, $\det(A_{\theta_0})$, $N(A_{\theta_0})$, a, b, $\gamma(A_{\theta_0})$, $card(S - S_0)$.*

19)Aller à 7.

Commentaires.

La 1^e partie conduit à la recherche d'une matrice A parfaite au-dessus de A_0, pour initialiser l'algorithme de Voronoï et le faire démarrer.

Pour bon nombre de réseaux étudiés, cette partie a été éxécutée d'abord seule.

Les étapes de la 2^e partie amènent aux différentes C-faces possibles.

À la ligne 9, la résolution du système (I) s'est faite par les formules de Cramer(on a utilisé les fonctions **det** de **gp**).

La 3^e partie est constituée des tests de contiguïté pour avoir les contigus de A relatifs

à la C-face. Les résultats sont recueillis dans un fichier ouvert au préalable, et qu'on a dénommé ici **resparf8**.

A la ligne 14, A_θ est en fait rendu entier et m est alors le minimum de bA_θ, c'est à dire bm.

Une fois connus les contigus de A, pour chercher les contigus de chacun d'eux , on peut faire commencer l'algorithme à la ligne 5 après introduction d'une nouvelle matrice (en fait on peut s'arranger pour introduire seulement la dernière colonne).

10 Algorithme de tri

À première vue ce chapitre est sans intérêt. Il n'en est rien. Laissons Conway-Sloane (c.f. [5] page 44) parler de K.C. Stacey (qui a travaillé en dimension 7):

«*Stacey's computer in fact generated all perfect septenary lattices, but unfortunately it produced thousands of Gram matrices, and Stacey was unable to decide just which pairs of these were equivalent...*»

Le mérite de Stacey est d'avoir quand même pu trouver les 33 réseaux parfaits en dimension 7 sans toutefois conclure à l'exhaustivité. C'est D.O. Jaquet qui l'a conclue grâce à son programme d'identification ... donnant ainsi naissance au programme **isom** de C. Batut, base de départ pour notre classement.

En effet, le même problème se pose dans notre cas. Dans le fichier **resparf8** les mêmes réseaux (à A_0-équivalence près) peuvent se répéter puisque des parties C distinctes peuvent engendrer la même face. De plus, on veut également les contigus des différents réseaux. Il est donc essentiel de distinguer ces réseaux, de les trier.

10.1 Tri des réseaux du fichier resparf8.

Soient t réseaux $R_1, R_2, ..., R_t$ dans le fichier **resparf8**; on veut les trier, ie ne conserver que ceux qui sont distincts à A_0-equivalence près. On ouvre un fichier **cresnouv8** dans lequel seront inscrits les contigus distincts de A. On procède alors de la manière suivante:

On compare R_i par **hisom** successivement à tous les réseaux R'_u de **cresnouv8**. Si R_i n'est H-isométrique à aucun des R'_u, c'est un nouveau réseau qu'on inscrit dans **cresnouv8** à la suite de ceux qui existent déja; (**cresnouv8** étant vide au départ, R_1 va s'écrire dedans initialement).

Puis on passe au réseau suivant R_{i+1}, et on itère la procédure ..., et ainsi de suite jusqu'à R_t.

Le fichier **cresnouv8** n'aura ainsi que les contigus distincts du réseau parfait A de matrice de Gram A. On sauve les données de **cresnouv8** dans un fichier **fActg** (la lettre **A** rappelle des résultats relatifs à la matrice A); puis on réalise les mêmes étapes pour

trier les réseaux de **cresnouv8** dans un fichier stable **resnouv8**, avant d'effacer ce qu'il y a dans **resparf8** et **cresnouv8**. Appliquant successivement à chacune des matrices A qu'on prend dans **resnouv8**, d'une part le programme **ctg**, d'autre part le programme de tri qu'on vient de décrire, on aura en définitive deux résultats:

-Tous les réseaux distincts Λ_i au-dessus de Λ_0 (qu'on trouvera dans **resnouv8**).

-Les contigus de chacun des Λ_i.

Regardons de plus près cet algorithme de tri qu'on appellera ici **dctg**.

10.1.1 Algorithme dctg.

1)[Initialisation] $T \longleftarrow 1$.

2)Créer fichier **F1**; *créer fichier* **F2**;

3)Créer fichier **cresnouv8**.

*4)***F1**$\longleftarrow$ **resparf8**; **F2** $\longleftarrow$ **cresnouv8**.

5)Chercher le nombre t de réseaux inscrits dans **F1**.

6)[Initialisation] $i \longleftarrow 1$.

7)Choisir R_i *dans* **F1**.

8)[Initialisation] $u \longleftarrow 1$.

9)Si (R'_u *n'éxiste pas dans* **F2**) *alors* $\{R'_u \longleftarrow R_i$; *inscrire* R'_u *dans* **F2**; *aller ligne 12*$\}$.

*10)[***hisom***]Comparer* $R_i et R'_u$ *par* **hisom**.

11)Si (R_i *non H-isométrique à* R'_u) *alors* $\{u \longleftarrow u+1$; *aller ligne 9*$\}$.

12)$i \longleftarrow i+1$; *si*$(i \neq t+1)$ *alors (aller ligne 8).*

13)Si (T=1) alors (afficher A,invariants de A, spect(A), les contigus de A qui sont dans **cresnouv8***).*

14)Si (fichier **resnouv8** *n'existe pas) le créer.*

15)Si (T=2) alors { **resnouv8** $\longleftarrow$ **F2**; *fin*}.

*16)***F1**$\longleftarrow$ **cresnouv8**; **F2**$\longleftarrow$ **resnouv8**.

17)T=2; aller ligne 5.

Commentaires.

La valeur 2 donnée à T à la ligne 17, empêche la ligne 13 de s'executer au 2^e tour. L'instruction *fin* de la ligne 15 n'est pas une fin en soi. Dans la pratique, on ouvre le fichier **resnouv8** et l'on prend un réseau non déja choisi qu'on traite en utilisant de nouveau **ctg**.

Les fichiers **resparf8**, **cresnouv8**, **resnouv8** sont des fichiers binaires; les programmes (**lfrp8**, **lfcrn8**, **lfrn8**) pour respectivement les lire et afficher le contenu à l'écran sont élémentaires.

11 Exemples

Les différentes étapes à suivre pour chercher par contiguïté les réseaux Λ au-dessus de Λ_0 se résument ainsi en manipulations:

1)Introduire A_0 pour éxécuter **depf**. Ceci a pour but de trouver la matrice A parfaite ayant un coin A_0.

2)Introduire A et lancer **ctg**. Il y a création du fichier **resparf8** pour recueillir les réseaux 'indistincts' contigus de Λ.

On fera de telle sorte de sauver dans le fichier **fActg** spect(A) et les invariants de A.

3)Trier les réseaux de **resparf8** grâce à **dctg**. Les contigus distincts (à H-isométrie près) de Λ s'inscrivent dans le fichier **cresnouv8**. En même temps la liste des réseaux au-dessus de Λ_0 prend forme dans le fichier **resnouv8**.

4)Le programme **lfcrn8** rajoute les contigus distincts dans le fichier **fActg**.

6)Ouvrir le fichier **resnouv8** (c'est le programme **lfrn8**) pour choisir une nouvelle matrice A qui n' a pas été traitée, et recommencer à l'étape 2.

Si toutes les matrices A sont traitées, présenter les résultats tels qu'on les voit sur la table.

Mieux vaut prendre des exemples tant il est vrai qu'un algorithme ne se comprend qu'en l'exécutant.

11.1 Premier exemple: Étude de $\Lambda_0 = P(7,2)$

1^e *manipulation* :

1)On lance **depf** après avoir introduit les coefficients de A_0.

2)Les éléments diagonaux ne sont pas tous égaux entre eux. Le programme **nvgram** va donner une nouvelle matrice de Gram A_0 qui est

$$A_0 = \begin{pmatrix} 3 & 1 & -1 & -1 & -1 & -1 & 1 \\ & 3 & 1 & -1 & -1 & -1 & -1 \\ & & 3 & 1 & -1 & -1 & -1 \\ & & & 3 & 1 & -1 & -1 \\ & & & & 3 & 1 & -1 \\ & & & & & 3 & 1 \\ & & & & & & 3 \end{pmatrix}.$$

3)Cherchons un réseau parfait Λ en dimension 8 qui contient Λ_0 et dont la matrice de Gram est de la forme

$$A = \begin{pmatrix} 3 & 1 & -1 & -1 & -1 & -1 & 1 & a \\ & 3 & 1 & -1 & -1 & -1 & -1 & b \\ & & 3 & 1 & -1 & -1 & -1 & c \\ & & & 3 & 1 & -1 & -1 & d \\ & & & & 3 & 1 & -1 & e \\ & & & & & 3 & 1 & f \\ & & & & & & 3 & g \\ & & & & & & & 3 \end{pmatrix},$$

i.e. écrite dans une base de vecteurs minimaux.

Les paramètres entiers a, b, c, d, e, f, g variant dans l'intervalle $[-\frac{3}{2}, \frac{3}{2}]$, c'est-à-dire dans $\{0, \pm 1\}$, on constate qu'il n'existe pas de réseaux parfaits de cette forme.

4)On renormalise à 6 la matrice A_0, et on fait varier alors les paramètres a, b, c, d, e, f, g dans $\{-3, -2, -1, 0, 1, 2, 3\}$, ie A aura pour allure:

$$A = \begin{pmatrix} 6 & 2 & -2 & -2 & -2 & -2 & 2 & a \\ & 6 & 2 & -2 & -2 & -2 & -2 & b \\ & & 6 & 2 & -2 & -2 & -2 & c \\ & & & 6 & 2 & -2 & -2 & d \\ & & & & 6 & 2 & -2 & e \\ & & & & & 6 & 2 & f \\ & & & & & & 6 & g \\ & & & & & & & 6 \end{pmatrix}$$

On recommence l'opération. Et cette fois le programme **depf** donne un réseau de départ Λ avec une matrice de Gram A ayant pour dernière colonne:

$$a = b = c = d = e = e = f = g = 1; \quad 8^e coefficient = 6$$

2^e *manipulation* :

5)Après avoir introduit A on lance **ctg**. L'ensemble $S(\Lambda)$ des vecteurs minimaux de Λ est affiché avec les invariants classiques (voir annexe III).

6)S_0 est repéré. On le remarque sur la liste: les 8^e composantes sont nulles. Il y en a 28 exactement (le cardinal de $S(\mathbb{E}_7^*)$).

7)$|S - S_0| = 16$; les dernières composantes de ces vecteurs ne sont pas nulles. Prendre une partie C à 7 éléments dans $S - S_0$.

Il y en a $\binom{16}{7} = 11440$.

8) 9) 10) 11) 12) Toutes ces lignes s'illustrent de la même manière que sur la partie $C = \{1, 2, 3, 4, 5, 6, 7\}$ de rang 7, où 1,2,3,4,5,6,7 sont les numéros des vecteurs minimaux de la liste. On a l'équation de la face $x_7 = 0$. $\sigma = 36$ (c'est 28+8).(voir annexe III).

Nous trouvons ainsi 70 C-faces , chacune avec un contigu, et tous ces contigus sont recueillis dans le fichier **resparf8** (voir annexe III).

En même temps les invariants de A et son spectre s'inscrivent dans le fichier ascii **fActg**.

3^e *manipulation* :

Cette partie consiste à trier les réseaux de **resparf8**. On exècute **dctg**. Le travail de classement s'opère comme on l'a expliqué au §10. On doit s'attendre à trouver les fichiers **cresnouv8** et **resnouv8**.

4^e *manipulation* :

On exécute le programme **lfcrn8**. Les contigus distincts de Λ, symbolisés par A, s'ajoutent à ceux qui éxistent déjà dans le fichier **fActg**.

C'est le réseau:

$$1, 1, 1, 1, 1, 1, -1, 6, 44, 20480, 6, 2, 1, 1734742, 16$$

(lire le sommaire de l'annexe II pour la signification).

5^e *manipulation* :

On ouvre le fichier **resnouv8**. On trouve le même réseau que précédemment. On recommence à l'étape 2. On s'aperçoit que la liste de **resnouv8** ne s'allonge pas. P(7,2) ne possède qu'un seul réseau parfait au-dessus de lui et qui est son propre contigu. Un résultat qui n'est pas sans surprendre. Le graphe de contiguité aura l'allure de la figure 3 (voir annexe IV).

On n'a plus qu'à mettre en forme les résultats.

Il est évident qu'en prenant une autre matrice A_0 équivalente à la première, on trouverait des résultats équivalents. C'est ce qui a été fait à l'annexe II pour P(7,2).

Temps machine: 3 minutes sur la station de travail **SPARC 2**.

11.2 Deuxième exemple : Étude de $\Lambda_0 = P(7,3)$.

On recommence le plan comme précédemment. On arrive à la liste finale de l'annexe II. On remarque que P(8,1;3) et P(8,2;3) ont les mêmes invariants classiques. Cependant leurs spectres les différencient. Le graphe de contiguité est à la figure 4 de l'annexe IV.

11.3 Troisième exemple.

Nous prenons au hasard P(7,5), P(7,26) et P(7,27) que nous étudions.

Pour information le temps-machine pour P(7,5) est de 3h 48mn.

Donnons sans commentaires les résultats à l'annexe II; voir aussi leurs graphes de contiguité (annexe IV, figures 5, 6, 7).

11.4 Quatrième exemple : Et les réseaux de racines?...

Et les réseaux de racines? Pourquoi n'ont-ils pas été étudiés?

Bien sûr que si! Un essai a été fait. Le programme a tourné pendant 10 jours sans résultats notables à part le réseau $\mathbb{L}$ de Barnes noté ici P(8,2;1) $\simeq$ P(8,2;33). Il faut signaler que $\mathbb{L}$ a été trouvé accidentellement en choisissant une partie C au hasard dans $S - S_0$ lors de l'étude de P(7,1)=$\mathbb{E}_7$.

En effet, comme on a pu le remarquer déjà, la ligne 7 de l'algorithme **ctg** fait choisir une partie C de n-1 éléments dans $S - S_0$. Pour les réseaux de racines qui nous préoccupent, si le cardinal de $S - S_0$ est égal à k (k est symbolisé par la variable rr dans notre programme informatique), alors il faut passer en revue $\binom{k}{7}$ combinaisons de vecteurs.

Portons-nous à l'annexe V et on comprendra pourquoi:

Pour P(8,1;1) k=57, $\binom{57}{7} = 264\ 385\ 836$;

pour P(8,1;4) k=78, $\binom{78}{7} = 2\ 641\ 902\ 120$;

pour P(8,1;33) k=92, $\binom{92}{7} = 8\ 760\ 554\ 088$;

pour P(8,2;33) k=43, $\binom{43}{7} = 32\ 224\ 114$;

Devant ces grands nombres qui font traîner en longueur le programme, nous avons préféré mettre les réseaux de racines de côté. Ils méritent à eux seuls une étude particulière plus approfondie. L'étude est donc incomplète comme l'illustre le graphe de contiguité de chacun de ces réseaux.

Le problème est donc toujours ouvert:

Quels sont les réseaux parfaits de dimension 8 au-dessus des réseaux de racines de dimension 7?

11.5 En guise de conclusions.

Malgré sa lourdeur, ce programme tel qu'il a été conçu a donné des satisfactions : il est à l'origine de l'aboutissement de la table, véritable herbier de réseaux parfaits en dimension 8. Conscients de pouvoir le rendre plus performant, nous avons été confrontés au compromis suivant:

ou bien perdre du temps-homme à rendre ce programme optimal, et alors on courrait le risque de s'éterniser sans voir le catalogue,

ou bien chercher les contigus tout en apportant des corrections au fur et à mesure que les "bugs" se présentent, et alors viendront les encouragements dûs aux premiers résultats.

On a choisi la 2^e solution. D'autant plus que les vérifications sont faciles à faire quand on suit pas à pas le travail. Le temps-machine n'a donc pas eu l'importance qu'il méritait dès lors que le catalogue prenait forme.

Mais ...

un programme n'est jamais terminé. Il n'y a pas de raison que le nôtre le soit. Toutes les portes restent ouvertes pour l'améliorer.

Bibliographie

[1] **A.Korkine, G.Zolotareff:** a)*Sur les formes quadratiques positives quaternaires.* Math. Ann. 5 (1872), 581-583.
b)*Sur les formes quadratiques.*Math. Ann. 6 (1873), 366-389.
c)*Sur les formes quadratiques positives.* Math. Ann. 11 (1877), 242-292.

[2] **E.S. Barnes:** a)*The perfect and extreme senary forms.* Canad. J. Math. 9 (1957), 235-242.
b)*On a theorem of Voronoï.* Proc. Cambridge Phil. Soc. 53 (1957), 537-539.

[3] **K.C. Stacey:** a)*The enumeration of perfect septenary forms.* J. London Math. Soc. 10 (1975), 97-104.
b)*The perfect septenary forms with* $D_4 = 2$. J. Austral. Math. Soc. 22 (1976), 144-164.

[4] **D.O. Jaquet:** a)*Domaines de Voronoï et algorithme de réduction des formes quadratiques définies positives.* Sem. Théorie des Nombres, Bordeaux 2 (1990), 163-215.
b)*Description des voisines de* $\mathbb{E}_7, \mathbb{D}_7, \mathbb{D}_8, \mathbb{D}_9$. Preprint (juin 1992).
c)*Thèse: Énumération complète des classes de formes parfaites en dimension 7.* Institut de Mathématiques et d'informatique, Université de Neuchâtel, 80 pages (1991).

[5] **J.H. Conway, N.J.A. Sloane:** a)*Low-dimensional lattices. III Perfect forms.* Proc. Royal Soc. London. A, 418 (1988), 43-80.
b)*Sphères Packings, Lattices and Groups .* Springer-Verlag, Grundlehren n^0 290, Heidelberg 1988.

[6] **A-M. Bergé, J. Martinet:** a)*Réseaux extrêmes pour un groupe d'automorphismes.* Astérisque 198-200 (1992), 41-66.

[7] **A-M. Bergé, J. Martinet, F. Sigrist:** *Une généralisation de l'algorithme de Voronoï.* Preprint.

[8] **G. Voronoï:** *Sur quelques propriétés des formes quadratiques positives parfaites.* J.Reine angew.Math. 133 (1908), 97-178; .

[9] **J. Martinet** *Réseaux parfaits des espaces euclidiens.* Ouvrage à paraître, édition provisoire du 9 juillet 1992.

[10] **A-M. Bergé** *Réseaux parfaits.* Cours inédit (DEA 1990-1991 , UFR Bordeaux I).