
Résolution numérique de l'équation eikonale par la méthode Fast-Marching

Thomas COURANT

Stage de L3 fait à l'Institut Mathématique de Toulouse,
encadré par Jérôme Fehrenbach.

Table des matières

1	Introduction	3
2	Résolution avec la méthode de Fast-Marching	3
2.1	Présentation du problème	3
2.2	Discrétisation du problème	4
2.3	Présentation théorique de l'algorithme Fast-Marching	6
2.4	Etude de l'opérateur discrétisé de Hopf-Lax sur une discrétisation quelconque	7
3	Algorithme Fast Marching avec une métrique fortement anisotropique	11
3.1	Principe de l'algorithme	11
3.2	Construction du voisinage	13
3.2.1	Construction d'une super-base M -obtus	15
3.2.2	Etude de l'algorithme de Lagrange	18
3.2.3	Présentation de l'algorithme en dimension 3	21
3.2.4	Etude de l'algorithme en dimension 3 et 4	22
3.3	Etude de l'algorithme FM-LBR	26

1 Introduction

Dans ce travail, nous nous intéressons à l'équation eikonale. C'est une équation aux dérivées partielles non linéaire et un cas particulier des équations d'Hamilton-Jacobi. On la retrouve dans des problèmes de propagation d'ondes, notamment en optique géométrique, car elle permet de décrire le chemin pris par la lumière dans un milieu. Sa résolution est aussi utile en traitement d'images, on peut notamment faire de la segmentation d'image avec, et/ou de la recherche de géodésique minimale. Ces différentes utilisations nous poussent à trouver un algorithme pour résoudre efficacement cette équation. Il existe plusieurs méthodes pour la résoudre comme les méthodes AGSI et Fast-Marching. Nous allons ici nous concentrer sur la méthode Fast-Marching car elle permet la résolution en ne passant qu'une fois sur chaque sommet.

2 Résolution avec la méthode de Fast-Marching

2.1 Présentation du problème

Le but de ce travail est de décrire une méthode permettant de résoudre numériquement l'équation eikonale en dimensions 2 et 3. Pour la suite posons $m \in \{2,3\}$, Ω une partie connexe bornée et on aura besoin d'une métrique riemannienne. Dans cette étude on considère que cette métrique riemannienne est juste une application $\mathcal{M} \in C^0(\overline{\Omega}, \mathbb{S}_m^+)$.

Le problème est donc le suivant, on cherche une fonction $u : \overline{\Omega} \rightarrow \mathbb{R}$ vérifiant :

$$\begin{cases} \|\nabla u(z)\|_{\mathcal{M}(z)^{-1}} = 1 & \text{si } z \in \Omega, \\ u(z) = 0 & \text{si } z \in \partial\Omega \end{cases} \quad (1)$$

Cette équation est donc une équation aux dérivées partielles non linéaires et notre objectif est de trouver une solution à ce problème. Or, une des difficultés vient du fait qu'il n'existe pas toujours une solution. Par exemple pour $m = 1$ et $\Omega = [0, 1]$, on se trouve avec le problème suivant :

$$\begin{cases} |f'(x)| = 1 & \text{si } x \in \Omega, \\ f(x) = 0 & \text{si } x \in \partial\Omega, \end{cases} \quad (2)$$

qui d'après le théorème de Rolle ne possède pas de solution (f' doit s'annuler au moins une fois). Ceci nous oblige à définir des solutions faibles du problème (1).

Definition 2.1. (*Solution de viscosité*)

$u \in C^0(\overline{\Omega})$ est une solution de viscosité de (1) si et seulement si :

1. Pour tout $\phi \in C^\infty(\Omega)$, si $x_0 \in \Omega$ est un maximum local de $u - \phi$ alors

$$\|\nabla\phi(x_0)\|_{\mathcal{M}(x_0)^{-1}} - 1 \leq 0 \quad (3)$$

2. Pour tout $\phi \in C^\infty(\Omega)$, si $x_0 \in \Omega$ est un minimum local de $u - \phi$ alors

$$\|\nabla\phi(x_0)\|_{\mathcal{M}(x_0)^{-1}} - 1 \geq 0 \quad (4)$$

Si u vérifie seulement (3) (respectivement (4)), alors u est une sous-solution (respectivement sur-solution) de viscosité.

Pour avoir une étude détaillée des solutions de viscosité dans un cadre plus général on peut se référer à ce cours (voir [1]). Mais ici seule cette définition nous intéresse car elle nous permet d'énoncer le théorème suivant, que l'on peut retrouver dans [2].

Théorème 2.1. (Existence et unicité de la solution de viscosité)

Il existe une et une seule solution de viscosité du problème (1). En notant u cette solution alors elle est donnée par la formule de Hopf-Lax :

$$\forall x \in \Omega, u(x) = \inf_{y \in \partial\Omega} (\delta(x, y)), \quad (5)$$

où

$$\delta(x, y) = \inf \left\{ \int_0^1 \|\xi'(t)\|_{\mathcal{M}(\xi(t))} dt \mid \xi \in C_{pm}^1(\overline{\Omega}) \text{ et } \xi(0) = x, \xi(1) = y \right\}.$$

C'est donc cette solution que nous allons devoir calculer numériquement. Le but de ce travail n'étant pas l'étude des solutions nous ne détaillerons pas plus ce théorème. Par contre, nous pouvons remarquer que $u(x)$ est simplement la longueur du plus court chemin reliant x à $\partial\Omega$.

2.2 Discrétisation du problème

La résolution se passe sur un espace discrétisé, c'est à dire qu'on considère qu'un nombre fini de points dans Ω que l'on notera Z . Dans cet espace lorsque nous parlerons de simplexe nous désignerons les triangles en dimension 2 et tétraèdres en dimension 3 dont les sommets appartiennent à Z et tel qu'il n'existe pas de points de Z qui se trouve dans son intérieur.

Pour la résolution, on va s'inspirer de l'algorithme de Dijkstra et du principe de variation locale. C'est à dire si, on considère $x \in \Omega$ et $V(x)$ un voisinage assez petit de x alors si l'on connaît u sur $\partial V(x)$ on peut calculer $u(x)$ grâce à la formule :

$$u(x) = \inf_{y \in \partial V(x)} \{u(y) + \delta(x, y)\}. \quad (6)$$

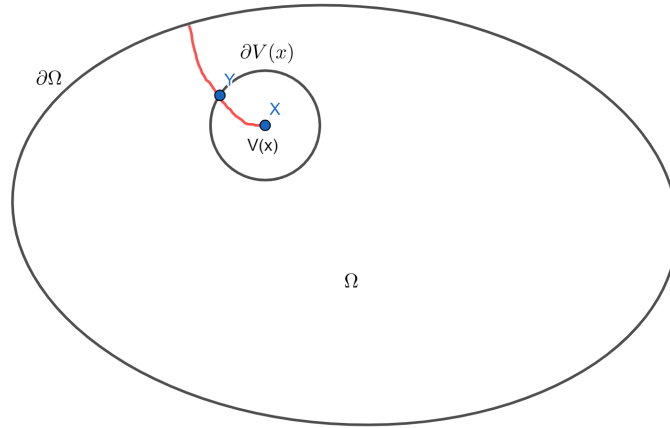


FIGURE 1 – Principe de variation locale

Et dans le cas où $V(x)$ est assez petit on peut approcher $\delta(x, y)$ par $\|x - y\|_{\mathcal{M}(x)}$. Ceci va nous permettre de définir l'opérateur de Hopf-Lax :

$$\Lambda(u)(x) = \inf_{y \in \partial V(x)} \{ \|x - y\|_{\mathcal{M}(x)} + u(y) \}$$

Dans le cas discrétisé, $V(x)$ correspond au polygone créé par tous les points voisins de x et on utilise une interpolation linéaire pour approcher la valeur de u sur $\partial V(x)$. Ainsi l'opérateur de Hopf-Lax discrétisé devient :

$$\Lambda(u)(x) = \min_{y \in \partial V(x)} \{ \|x - y\|_{\mathcal{M}(x)} + I_{V(x)} u(y) \} \quad (7)$$

où I_V est l'interpolation linéaire sur V . Par exemple en dimension 2, $V(x)$ correspond au polygone suivant :

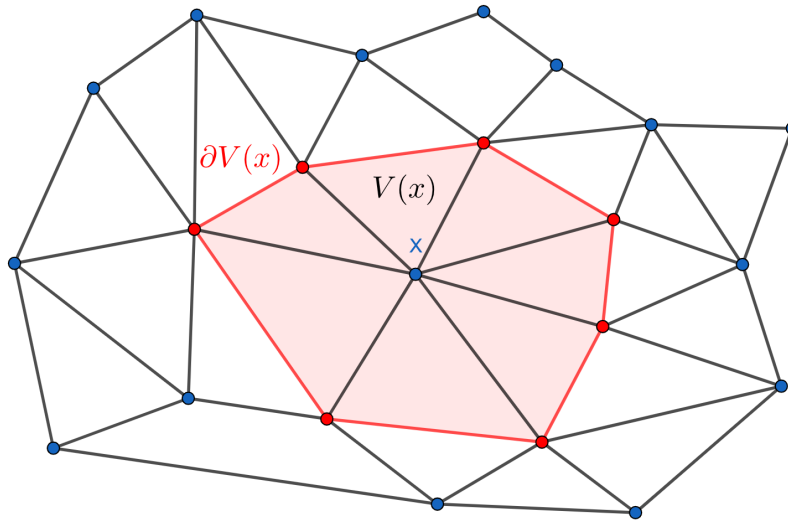


FIGURE 2 – Voisinage en dimension 2

En notant $T(x)$ l'ensemble des simplexes de $V(x)$ dont x est un sommet on a :

$$\Lambda(u)(x) = \min_{\tau \in T(x)} \left\{ \min_{s \in [0,1]} \|(1-s)a + sb\|_{\mathcal{M}(x)} + (1-s)u(a) + su(b) \mid (x, a, b) \text{ étant les sommets de } \tau \right\} \quad (8)$$

Et en dimension 3, les simplexes sont sous la forme d'un tétraèdre, en posant $\tau \in T(x)$ on définit $B_\tau(x)$ le triangle du tétraèdre dont x n'est pas un des sommets, on a donc :

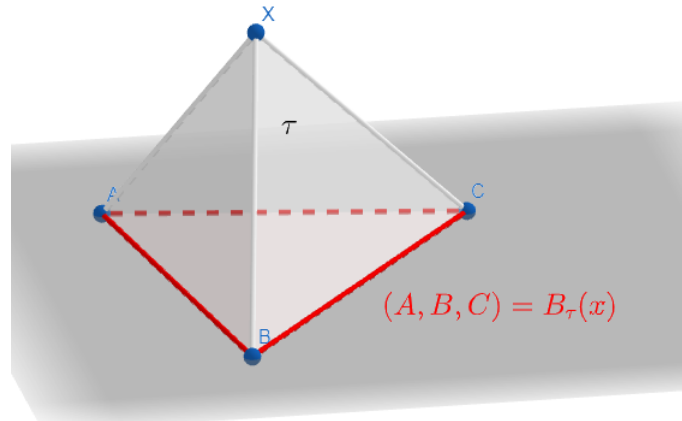


FIGURE 3 – Simplexe en dimension 3

Et l'opérateur discrétisé de Hopf-Lax est le suivant pour $m = 3$:

$$\Lambda(u)(x) = \min_{\tau \in T(x)} \min_{y \in B_\tau(x)} \left\{ \|x - y\|_{\mathcal{M}(x)} + I_{B_\tau(x)} u(y) \right\} \quad (9)$$

où $I_{B_\tau(x)} u(y)$ est une interpolation linéaire en fonction des valeurs prises par u sur les sommets du triangle $B_\tau(x)$. De manière générale, on pose $\varphi_\tau^u(x)$ pour $m \in \{2, 3\}$ de telle manière à ce que $\Lambda(u)(x) = \min_{\tau \in T(x)} \varphi_\tau^u(x)$.

Finalement notre objectif est donc de résoudre le problème de point fixe suivant :

$$\begin{cases} u(z) = \Lambda(u)(z) & \text{si } z \in Z \cap \Omega \\ u(z) = 0 & \text{si } z \in Z \setminus \Omega \end{cases} \quad (10)$$

On va maintenant montrer avec quelles conditions sur Λ on va pouvoir résoudre ce problème de point fixe grâce à la méthode de Fast-Marching.

2.3 Présentation théorique de l'algorithme Fast-Marching

Dans cette sous-section notons X un ensemble fini, $U \in \mathcal{U} :=]-\infty, \infty]^X$ et $\Gamma : \mathcal{U} \leftarrow \mathcal{U}$ une fonction. Le but est de résoudre :

$$\Gamma(U) = U. \quad (11)$$

Cette étude se base sur l'annexe B du travail [3] de Jean-Marie Mirebeau.

On introduit aussi les notations suivantes :

- Pour $U, V \in \mathcal{U}$ on note $U \leq V$ si pour tout $x \in X$, $U(x) \leq V(x)$.
- Pour $U \in \mathcal{U}$ et $\lambda \in [-\infty, +\infty]$ on définit $U^{<\lambda} \in \mathcal{U}$ par :

$$U^{<\lambda} = \begin{cases} U(x) & \text{si } U(x) < \lambda, \\ +\infty & \text{sinon,} \end{cases}$$

de même pour $U^{\leq\lambda}$.

- Pour $U \in \mathcal{U}$ et $A \subset X$ on définit $U^A \in \mathcal{U}$ par :

$$U^A = \begin{cases} U(x) & \text{si } x \in A, \\ +\infty & \text{sinon.} \end{cases}$$

Nous pouvons maintenant définir certaines propriétés de l'opérateur Γ .

Définition 2.2. (*Monotonie et causalité*)

X est un ensemble fini, $\mathcal{U} =]-\infty, \infty]^X$ et on considère une fonction $\Gamma : \mathcal{U} \rightarrow \mathcal{U}$. Elle est dite

1. *Monotone*, si pour tout $U, V \in \mathcal{U}$ telle que $U \leq V$ alors $\Gamma(U) \leq \Gamma(V)$.
2. *Causale*, si pour tout $U, V \in \mathcal{U}$ et $\lambda \in]-\infty, \infty]$ tel que $U^{<\lambda} = V^{<\lambda}$ alors $(\Gamma U)^{\leq\lambda} = (\Gamma V)^{\leq\lambda}$

On peut donc énoncer le théorème suivant qui nous dit simplement que si Γ est monotone et causale alors on peut résoudre (11) en seulement $|X|$ itérations.

Théorème 2.2. (*Fast-Marching*)

On suppose Γ monotone et causale. On pose $N = |X|$, $A_0 = \emptyset$ et $U_0 \in \mathcal{U}$ la fonction qui prend la valeur $+\infty$ sur X . Pour $1 \leq i \leq N+1$, on définit :

1. $U_i = \Gamma(U_{i-1}^{A_{i-1}})$,
2. $A_i = A_{i-1} \cup \{x_i\}$ où x_i minimise U_i sur $X \setminus A_{i-1}$.

Alors $\Gamma U_N = U_N$. De plus $U_{i+1}^{A_i} = U_i^{A_i}$ pour $0 \leq i \leq N$.

Démonstration. Soit $\lambda_0 = -\infty$ et $\lambda_i = U_i(x_i)$ pour $1 \leq i \leq N$.

Dans un premier temps nous allons montrer par récurrence sur $i \in \llbracket 0 ; N \rrbracket$ la propriété :

$$\mathbb{P}_i : U_{i+1}^{\leq\lambda_i} = U_i^{\leq\lambda_i} \text{ et } \lambda_i \leq \lambda_{i+1}. \quad (12)$$

Pour $i = 0$, alors $U_{i+1}^{\leq\lambda_i}$ et $U_i^{\leq\lambda_i}$ sont identiquement égales à $+\infty$ sur X , et comme $\lambda_0 = -\infty$, on a forcément $\lambda_0 \leq \lambda_1$.

Pour $i \in \llbracket 0 ; N-1 \rrbracket$ on suppose vrai \mathbb{P}_j pour $j \leq i$ et on veut montrer \mathbb{P}_{i+1} . Nous allons commencer par montrer que $(U_i^{A_i})^{<\lambda_i} = (U_{i-1}^{A_{i-1}})^{<\lambda_i}$, pour cela on considère $x \in X$ et on distingue deux cas :

- Si $x \in A_{i-1}$ alors il existe $j \leq i-1$ tel que $x_j = x$ et donc $U_j(x) = \lambda_j$. Or par hypothèse de récurrence (12) $\lambda_j \leq \lambda_{j+1} \leq \dots \leq \lambda_{i-1}$ et de plus $U_j^{\leq\lambda_j} = \dots = U_{i-1}^{\leq\lambda_j} = U_i^{\leq\lambda_j}$. Donc $U_{i-1}(x) = U_i(x) = \lambda_j$ et donc

$$(U_i^{A_i})^{<\lambda_i}(x) = (U_{i-1}^{A_{i-1}})^{<\lambda_i}(x) = \begin{cases} \lambda_j & \text{si } \lambda_j < \lambda_i, \\ +\infty & \text{sinon.} \end{cases}$$

— Si $x \notin A_{i-1}$, alors $U_i(x) \leq \lambda_i$ par définition de λ_i (2) donc

$$\left(U_i^{A_i} \right)^{<\lambda_i}(x) = \left(U_{i-1}^{A_{i-1}} \right)^{<\lambda_i}(x) = +\infty$$

On a donc bien $\left(U_i^{A_i} \right)^{<\lambda_i} = \left(U_{i-1}^{A_{i-1}} \right)^{<\lambda_i}$, par causalité de Γ , on obtient :

$$\left(\Gamma U_i^{A_i} \right)^{\leq \lambda_i} = \left(\Gamma U_{i-1}^{A_{i-1}} \right)^{\leq \lambda_i} \text{ donc } U_{i+1}^{\leq \lambda_i} = U_i^{\leq \lambda_i} \text{ par 1.}$$

Par l'absurde supposons $\lambda_{i+1} \leq \lambda_i$ on a alors $U_i(x_{i+1}) = U_i^{\leq \lambda_i}(x_{i+1}) = U_{i+1}^{\leq \lambda_i}(x_{i+1}) = \lambda_{i+1} < \lambda_i = U_i(x_i)$. Or x_i minimise U_i sur $X \setminus A_{i-1}$ et $x_{i+1} \in \setminus A_i \subset \setminus A_{i-1}$. Ainsi par l'absurde $\lambda_i \leq \lambda_{i+1}$ et on a démontré la propriété \mathbb{P}_{i+1} .

Ainsi U_i prend les valeurs $\{\lambda_1 \leq \dots \leq \lambda_i\}$ sur A_i et donc $U_{i+1}^{A_i} = U_i^{A_i}$ car $U_{i+1}^{\leq \lambda_i} = U_i^{\leq \lambda_i}$. Avec $i = N$ comme $A_N = X$ on obtient $U_N = U_{N+1} = \Gamma U_N$. \square

Dans le cas où Γ est seulement monotone, on peut quand même calculer numériquement la solution de (11) grâce à la méthode de Gauss-Seidel. On retrouve ce résultat dans l'annexe B de [3].

Le but maintenant va être d'étudier l'opérateur discrétisé de Hopf-Lax, pour trouver à quelles conditions il vérifie la définition 2.2.

2.4 Etude de l'opérateur discrétisé de Hopf-Lax sur une discrétisation quelconque

On commence en se plaçant en dimension 2 et, comme on l'a vu, l'opérateur de Hopf-Lax devient :

$$\Lambda(u)(x) = \min_{\tau \in T(x)} \left\{ \min_{s \in [0,1]} \left\| (1-s)a + sb \right\|_{\mathcal{M}(x)} + (1-s)u(a) + su(b) \mid (x, a, b) \text{ étant les sommets de } \tau \right\},$$

où $V(x)$ correspond au polygone créé par tous les points voisins de x et $T(x)$ à l'ensemble des simplexes de $V(x)$ dont x est un sommet.

On considère un point C de Z et on cherche à calculer :

$$\varphi_T^u(C) = \min_{s \in [0,1]} \left\{ \left\| (1-s)A + sB \right\|_{\mathcal{M}(C)} + (1-s)u(A) + su(B) \right\} \quad (13)$$

où T est un simplexe dont les sommets sont (A, B, C) .

On peut considérer ce problème géométriquement, pour cela on pose $s^* \in [0, 1]$ tel que

$$\varphi_T^u(C) = \left\| (1-s^*)A + s^*B \right\|_{\mathcal{M}(C)} + (1-s^*)u(A) + s^*u(B).$$

Ainsi en posant $u(C) = \varphi_T^u(C)$ et en considérant u comme affine dans le triangle (A, B, C) on peut tracer les équipotentielles de u et on obtient :

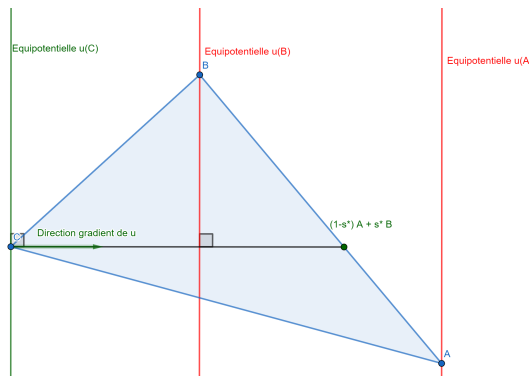


FIGURE 4 – Equipotentielles dans le triangle (A, B, C)

On peut remarquer que comme les valeurs extrêmes possibles pour s sont 0 et 1, si l'angle \widehat{ACB} est aigu ou droit les cas extrêmes sont les suivants :

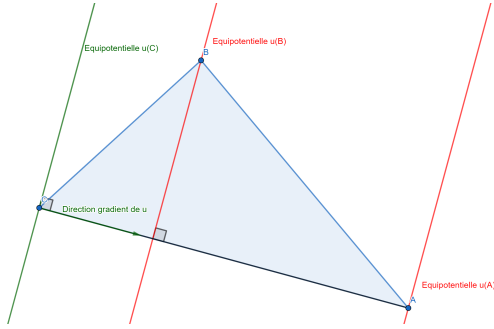


FIGURE 5 – Angle aigu et $s^* = 0$

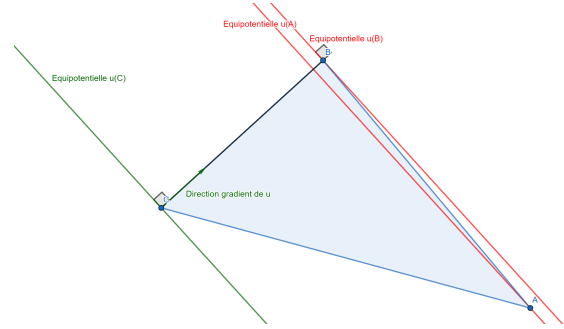


FIGURE 6 – Angle aigu et $s^* = 1$

Ainsi pour un angle \widehat{ACB} aigu ou droit, on a la majoration $\varphi_T^u(C) > \max(u(A), u(B))$. Dans le cas où l'angle est obtus, les cas limites deviennent :

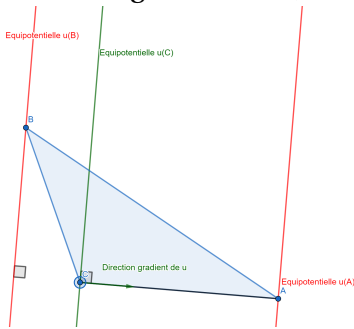


FIGURE 7 – Angle obtus et $s^* = 0$

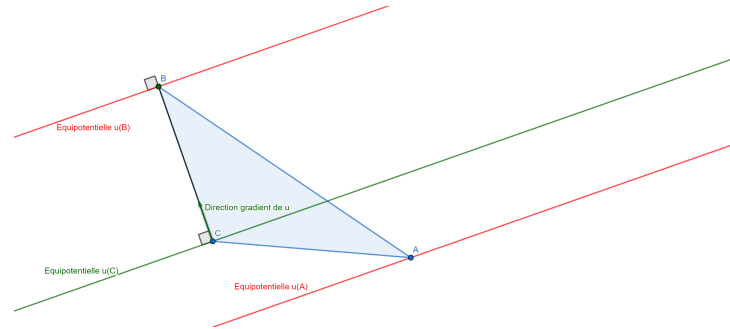


FIGURE 8 – Angle obtus et $s^* = 1$

On obtient qu'en dimension 2 que, si pour chaque simplexe T dont les sommets sont (A, B, C) , l'angle \widehat{ACB} est aigu ou droit pour $\langle \cdot | \cdot \rangle_{\mathcal{M}(C)}$ alors pour $C \in Z$ il existe un simplexe T dont les sommets sont (A, B, C) et tel que :

$$\Lambda(u)(C) = \varphi_T^u(C) > \max(u(A), u(B)). \quad (14)$$

Dans le cas $m = 3$, les simplexes sont des tétraèdres en imposant les mêmes conditions, les angles doivent être aigus ou droits, on obtient la même majoration. Pour le voir, il suffit de raisonner dans le simplexe T qui réalise le minimum de

$$\Lambda(u)(C) = \min_{\tau \in T(C)} \min_{y \in B_\tau(x)} \left\{ \|x - y\|_{\mathcal{M}(x)} + I_{B_\tau(x)} u(y) \right\},$$

et de considérer les triangles contenant le point y réalisant le deuxième minimum.

Pour conclure pour $m = \{2, 3\}$ en imposant les conditions précédentes, pour tout $C \in Z$ il existe un simplexe T dont les sommets sont (C, A_1, \dots, A_m) et tel que :

$$\Lambda(u)(C) = \varphi_T^u(C) > \max_{1 \leq i \leq m} u(A_i) \quad (15)$$

On va pouvoir montrer grâce à ce résultat que sous ces conditions que l'opérateur Λ vérifie la définition 2.2.

Théorème 2.3. *On suppose que tous les simplexes ont des angles aigus ou droits donc l'opérateur de Hopf-Lax est causal et monotone.*

Démonstration. Monotonie : Soit $u, v \in \mathcal{U}$ tel que $u \leq v$. Pour $C \in Z$ et T un simplexe dont C est un des sommets, comme $u \leq v$ alors $\varphi_T^u(C) \leq \varphi_T^v(C)$, donc $\Lambda(u) \leq \Lambda(v)$.

Causalité : Soit $u, v \in \mathcal{U}$ et $\lambda \in]-\infty, +\infty]$, on suppose que $u^{<\lambda} = v^{<\lambda}$. Soit $C \in Z$ et T un simplexe

telle que $\Lambda(u)(C) = \varphi_T^u(C)$.

Tout d'abord supposons que $\Lambda(u)(C) \leq \lambda$, ainsi en notant (A_1, \dots, A_m) les autres sommets de T on sait d'après (15) que $\max_{1 \leq i \leq m} u(A_i) < \lambda$ or $u^{<\lambda} = v^{<\lambda}$, ainsi on en déduit que pour tout $1 \leq i \leq m$, $u(A_i) = v(A_i)$.

On a donc $\varphi_T^u(C) = \varphi_T^v(C)$ qui implique que $\Lambda(v)(C) \leq \Lambda(u)(C) \leq \lambda$. Or par symétrie comme $\Lambda(v)(C) \leq \lambda$, on a $\Lambda(v)(C) \geq \Lambda(u)(C)$, on a donc l'égalité

$$\Lambda(v)(C) = \Lambda(u)(C).$$

Et si $\Lambda(u)(C) > \lambda$ on a par contraposée de ce qu'on a montré, $\Lambda(v)(C) > \lambda$ et donc $\Lambda(v)(C) = \Lambda(u)(C) = +\infty$.

On a donc montré que $(\Lambda(u))^{\leq \lambda} = (\Lambda(v))^{\leq \lambda}$ □

On peut donc donner l'algorithme pour résoudre le problème (10), en utilisant le principe du théorème 2.2.

Algorithm 1 Fast-Marching

Require: La valeur de la métrique $\mathcal{M}(z)$ pour $z \in Z \cap \Omega$.

Ensure: La fonction $u : Z \rightarrow \mathbb{R}$.

- 1: Initialiser la fonction u avec $+\infty$ sur $Z \cap \Omega$ et 0 sinon.
 - 2: Initialiser $b : Z \rightarrow \{\text{à traiter}, \text{accepté}\}$ en posant $b(z) \leftarrow \text{à traiter}$ pour tout $z \in Z$.
 - 3: **while** Il existe $y \in Z$ tel que $b(y) = \text{à traiter}$. **do**
 - 4: Soit y un point à *traiter* qui minimise u , on pose $b(y) \leftarrow \text{accepté}$.
 - 5: Pour tout x voisin de y tel que $b(x) = \text{à traiter}$, on calcule $u(x)$ en posant $u(x) \leftarrow \min \{u(x), \Lambda(u, x, b, y)\}$.
 - 6: **end while**
-

où $\Lambda(d, x, b, y)$ est l'opérateur discrétisé de Hopf-Lax (7), où on ne considère les simplexes qui ont pour sommet y et dont les autres sommets sont acceptés.

Par rapport au théorème 2.2, A_i correspond à l'ensemble des points considérés comme *accepté* et U_i la fonction u après i passage dans la boucle **while**. Comme d'après ce théorème on sait que $U_{i+1}^{A_i} = U_i^{A_i}$, il n'est pas nécessaire de calculer $\Lambda(u)$ sur les sommets déjà acceptés. De plus, le minimum $\lambda_i = U_i(x_i)$ ne se trouve que dans les voisins directs de l'ensemble des points acceptés. Ainsi à l'étape 5 on peut seulement calculer $\Lambda(u)$ pour les points voisins où on ne considère que les simplexes qui ont les autres sommets acceptés.

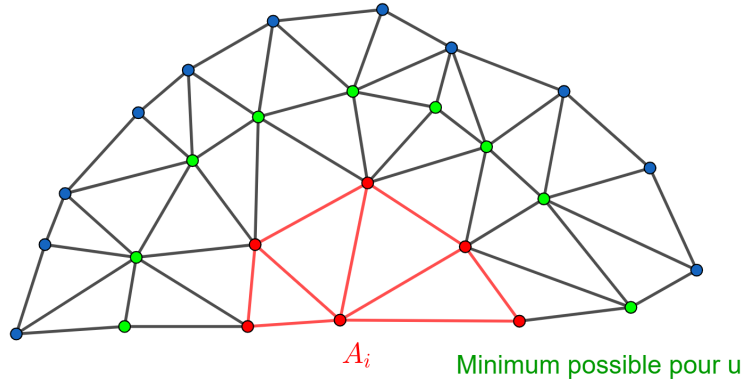


FIGURE 9 – Principe de l'algorithme

Au niveau de la complexité temporelle, on ne fait que N passages dans la boucle **while**. De plus en utilisant un tas pour sauvegarder les points qui sont à *traiter*, il peut être trié en $\mathcal{O}(\ln N)$, d'où une complexité globale pour cet algorithme en $\mathcal{O}(N \ln N)$. De plus, d'après le théorème 11 dans [2], nous avons la convergence de la solution calculée ici vers la solution de viscosité. Nous ne détaillerons pas ce point ici, en effet j'ai fait le choix d'étudier le cas où la métrique joue un rôle plus important. Et nous démontrerons dans cette deuxième partie des résultats intermédiaires de convergence.

3 Algorithme Fast Marching avec une métrique fortement anisotrope

L'étude précédente nous imposait une condition assez forte sur la discrétisation que l'on utilise pour pouvoir résoudre le problème efficacement avec la méthode de Fast-Marching. L'objectif ici va être de trouver un moyen pour pouvoir toujours utiliser cette méthode même si la métrique est fortement anisotrope, pour réussir nous allons devoir prendre pour discrétisation un réseau. Cet algorithme appelé FM-LBR (Fast-Marching and Lattice Base Reduction) a été développé dans cet article [4] par Jean-Marie Mirebeau.

3.1 Principe de l'algorithme

Comme précédemment, le but est de résoudre l'équation eikonale sur un domaine borné Ω , c'est à dire résoudre le problème suivant :

$$\begin{cases} \|\nabla D(z)\|_{M(z)^{-1}} = 1 & \text{si } z \in \Omega \\ D(z) = 0 & \text{si } z \in \partial\Omega \end{cases} \quad (16)$$

Ainsi le problème numérique à résoudre reste le même, que l'on peut formuler sous cette forme, où l'inconnue à trouver est la fonction d , et Z représente l'ensemble des points pris en compte.

$$\begin{cases} d(z) = \Lambda(d)(z) & \text{si } z \in Z \cap \Omega \\ d(z) = 0 & \text{si } z \in Z \setminus \Omega \end{cases} \quad (17)$$

et $\Lambda(d, z) = \min_{y \in \partial V(z)} \left\{ \|z - y\|_{M(z)} + I_{V(z)} d(y) \right\}$ est l'opérateur de Hopf-Lax et I_V est l'interpolation linéaire sur V .

Or dans cette partie la métrique va jouer un rôle plus important, en effet le but étant de résoudre ce système même lorsque la métrique est fortement anisotrope. Pour quantifier cela, on va devoir définir une grandeur importante, pour $M \in \mathbb{S}_m^+$ on définit

$$\kappa(M) = \sqrt{\|M\| \|M^{-1}\|} = \max_{\|u\|=\|v\|=1} \frac{\|u\|_M}{\|v\|_M}$$

Comme pour l'algorithme de Fast-Marching 1, l'objectif est de résoudre le problème en ne faisant qu'un seul passage sur tous les sommets. La solution est de choisir plus intelligemment les voisins à prendre en compte lors de la résolution de chaque sommet de manière à ce que les simplexes soient compatibles avec la métrique. Pour cela, le but va être pour chaque sommet de sélectionner les points autour de lui que l'on va prendre en compte comme ses voisins. L'algorithme est donc très similaire à 1, et est le suivant :

Algorithm 2 FM-LBR

Require: La valeur de la métrique $\mathcal{M}(z)$ pour $z \in Z \cap \Omega$.

Ensure: La fonction $d : Z \rightarrow \mathbb{R}$.

- 1: Pour tout $y \in Z$ on construit le voisinage $V(y)$ grâce à $\mathcal{M}(y)$.
 - 2: Et on pose $V[y] = \{z \in Z \cap \Omega, y \in V(z)\}$.
 - 3: Initialiser la fonction d avec $+\infty$ sur $Z \cap \Omega$ et 0 sinon.
 - 4: Initialiser $b : Z \rightarrow \{\text{à traiter}, \text{accepté}\}$ avec $b(z) \leftarrow \text{à traiter}$.
 - 5: **while** Il existe $y \in Z$ tel que $b(y) = \text{à traiter}$. **do**
 - 6: Soit y un point à *traiter* qui minimise d , on pose $b(y) \leftarrow \text{accepté}$.
 - 7: Pour tout $x \in V[y]$, on calcule $d(x)$ en posant $d(x) \leftarrow \min\{d(x), \Lambda(d, x, b, y)\}$.
 - 8: **end while**
-

Où $\Lambda(d, x, b, y)$ est une modification de l'opérateur de Hopf-Lax où l'on cherche le minimum sur les faces de $\partial V(x)$ qui contiennent y et dont tous les sommets sont *accepté*.

Dans l'algorithme de la première partie, on prend en compte naïvement les voisins pour chaque x , ici nous devons être plus précis pour que notre algorithme fonctionne encore même avec des métriques fortement anisotropiques. Le but dans la suite de ce travail va donc être de détailler la construction de ce voisinage et de ses propriétés.

Pour cela, nous allons restreindre l'étude dans le cas où Z est une partie finie d'une grille cartésienne en dimension 2 ou 3. C'est à dire nous partons du réseau \mathbb{Z}^m (avec $m = 2$ ou $m = 3$) auquel nous pouvons appliqué une rotation R , un changement d'échelle $h > 0$ et/ou un décalage grâce à $\xi \in \mathbb{R}^m$. C'est à dire que nous pouvons écrire que :

$$Z \subset hR(\xi + \mathbb{Z}^m) := \{hR(\xi + z) \mid z \in \mathbb{Z}^m\}. \quad (18)$$

Ainsi nous étudierons l'algorithme dans le cas où $Z \subset \mathbb{Z}^m$ et nous pourrons simplement résoudre dans le cas plus général où on a (18).

Mais pour commencer nous devons énoncer quelques résultats et définitions sur les réseaux. Nous trouverons dans ce cours [5] une étude détaillée des réseaux, ici nous donnerons la définition suivante.

Definition 3.1. (*Réseau*)

Soit $e = (e_1, \dots, e_m)$ une famille libre de vecteurs de \mathbb{R}^m , le réseau engendré par (e_1, \dots, e_m) est le sous groupe :

$$L(e) = \{z_1 e_1 + \dots + z_m e_m \mid \text{où } z_1, \dots, z_m \in \mathbb{Z}\}.$$

Lorsqu'on parle de \mathbb{Z}^m on parle du réseau engendré par la base canonique de \mathbb{R}^m .

On peut donc légitimement se demander à quelles conditions deux familles de vecteurs engendrent et le même réseau. C'est l'objectif de la proposition suivante pour cela nous introduisons un ensemble :

$$\text{GL}_m(\mathbb{Z}) = \{M \in \text{M}_m(\mathbb{Z}) \mid \exists N \in \text{M}_m(\mathbb{Z}), MN = I_m\}.$$

Proposition 3.1. On note $e = (e_1, \dots, e_m)$, $f = (f_1, \dots, f_m)$ deux familles libres de \mathbb{R}^m et on note $P = \text{Mat}_e(f_1, \dots, f_m)$.

1. $\text{GL}_m(\mathbb{Z}) = \{M \in \text{M}_m(\mathbb{Z}) \mid \det(M) = \pm 1\}$.
2. e et f engendrent le même réseau si et seulement si $P \in \text{GL}_m(\mathbb{Z})$.

Démonstration. Tout d'abord soit $M, N \in \text{M}_m(\mathbb{Z})$ tel que $MN = I_m$ alors $\det(M)\det(N) = 1$ or $\det(M)\det(N) \in \mathbb{Z}$ donc $\det(M) = \pm 1$.

Réciproquement on sait que $M^t \text{Co}(M) = \det(M) I_m$ or ${}^t \text{Co}(M) \in \text{M}_m(\mathbb{Z})$ donc si $\det(M) = \pm 1$ on a bien $M^{-1} = {}^t \text{Co}(M) \det(M)^{-1} \in \text{M}_m(\mathbb{Z})$.

Montrons l'autre point, dans un premier temps remarquons que les vecteurs de f appartiennent à $L(e)$ si et seulement si $P \in \text{M}_m(\mathbb{Z})$. De même en notant $Q = \text{Mat}_f(e_1, \dots, e_m)$, les vecteurs de e appartiennent à $L(f)$ si et seulement si $Q \in \text{M}_m(\mathbb{Z})$. Or on sait que $QP = I_m$ (e et f sont des bases de \mathbb{R}^m), ainsi e et f engendrent le même réseau si et seulement si $P \in \text{GL}_m(\mathbb{Z})$. \square

La dernière définition qu'il nous reste à donner est celle de cellule de Voronoï. Cela implique de munir \mathbb{R}^d d'une norme.

Definition 3.2. Soit $M \in \mathbb{S}_m^+$, e une famille libre de \mathbb{R}^m et $L(e)$ le réseau engendré on définit la cellule de Voronoï comme étant :

$$\text{Vor}_M(e) = \left\{ x \in \mathbb{R}^d \mid \forall v \in L(e), \|x - v\|_M \geq \|x\|_M \right\}.$$

C'est l'ensemble des vecteurs de \mathbb{R}^d qui sont plus proches de 0 que de n'importe quel autre vecteur du réseau pour la norme $\|\cdot\|_M$.

Nous pouvons donc maintenant nous intéresser à la construction des voisinages pour l'algorithme FM-LBR (2).

3.2 Construction du voisinage

Pour construire $V(x)$ l'objectif est de trouver \mathcal{T} un maillage qui couvre l'origine est en accord avec $\mathcal{M}(x)$ et de poser $V(x) = x + \mathcal{T}$. Comme on a vu dans la partie précédente pour que l'on puisse résoudre le problème de point fixe (17) avec un seul passage sur chaque sommet, il faut que Λ soit causale. Et donc, comme on l'a vu dans la première partie, ceci impose une condition sur les angles des simplexes composant le maillage.

Definition 3.3. (*M*-maillage)

Soit $M \in \mathbb{S}_m^+$ et \mathcal{T} un maillage (ensemble fini de points de \mathbb{Z}). Alors \mathcal{T} est un *M*-maillage si et seulement s'il couvre un voisinage de l'origine et pour tout simplexe T de \mathcal{T} dont les sommets sont v_0, \dots, v_m on a :

1. $v_0 = 0$ (quitte à intervertir les sommets)
2. (v_1, \dots, v_m) est une base de \mathbb{Z}^m et $|\det(v_1, \dots, v_m)| = 1$.
3. Pour tout $1 \leq i, j \leq m$, on a $\langle v_i | M v_j \rangle \geq 0$.

Pour ce donner une idée voici un *M*-maillage calculé en dimension 2, en orange on retrouve la boule unité pour la norme $\|\cdot\|_M$:

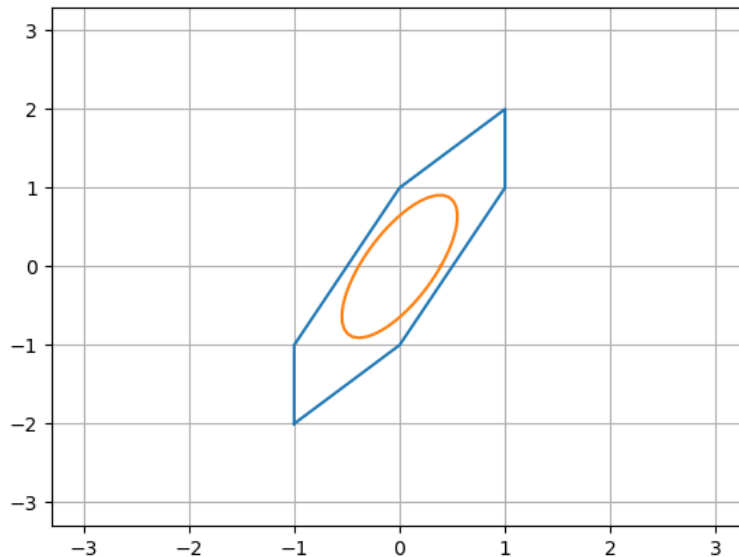


FIGURE 10 – Maillage en dimension 2

Si le maillage respecte cette définition alors d'après notre étude dans la partie précédente Λ sera causale et on pourra résoudre (17) avec un seul passage sur chaque sommet.

Grâce à la proposition suivante, on peut voir que si notre maillage ne vérifie pas 3, alors si $\kappa(M)$ est assez petit il sera quand même un *M*-maillage.

Proposition 3.2. Soit \mathcal{T} un maillage vérifiant les conditions de la définition 3.3 sauf la condition 3. Alors pour $M \in \mathbb{S}_m^+$ tel que $\kappa(M) \leq \Gamma(\mathcal{T})$, \mathcal{T} est un M -maillage et on définit :

$$\Gamma(\mathcal{T}) := \sqrt{\frac{1 + \gamma(\mathcal{T})}{1 - \gamma(\mathcal{T})}} \text{ où } \gamma(\mathcal{T}) = \min \left\{ \frac{\langle u|v \rangle}{\|u\| \|v\|}, \text{ avec } u \text{ et } v \text{ sommets commun non nul d'un simplexe } T \right\}$$

Démonstration. On considère un maillage \mathcal{T} et $M \in \mathbb{S}_m^+$ vérifiant les conditions nécessaires, il nous faut montrer 3, ainsi on note T un simplexe de \mathcal{T} et u, v deux de ces sommets.

Avec $u' = \frac{u}{\|u\|}$ et $v' = \frac{v}{\|v\|}$ on a $\|u' + v'\|^2 \geq 2(1 + \gamma(\mathcal{T}))$ et $\|u' - v'\|^2 \leq 2(1 - \gamma(\mathcal{T}))$.

On suppose $\langle u|Mv \rangle < 0$ c'est à dire $\|u' + v'\| < \|u' - v'\|$, ainsi

$$\kappa(M)^2 \geq \frac{\|u' - v'\|_M^2 \|u' + v'\|^2}{\|u' - v'\|^2 \|u' + v'\|_M^2} > \frac{1 + \gamma(\mathcal{T})}{1 - \gamma(\mathcal{T})}$$

donc $\kappa(M) > \Gamma(\mathcal{T})$, par contraposée on a le résultat voulu. \square

Ce résultat nous montre que dans le cas d'une discrétisation par un réseau, si la métrique est faiblement anisotrope, la méthode déployée dans la première partie est suffisante pour la résolution de l'équation.

La construction d'un M -maillage repose sur l'utilisation d'une base particulière qui est adaptée aux propriétés géométriques de la métrique.

Definition 3.4. (*Super-base*)

Soit $(e_0, \dots, e_m) \in (\mathbb{Z}^m)^{m+1}$, (e_0, \dots, e_m) est une super-base si et seulement si,

- $e_0 + \dots + e_m = 0$,
- (e_1, \dots, e_m) est une base de \mathbb{Z}^m et $|\det(e_1, \dots, e_m)| = 1$.

De plus, soit $M \in \mathbb{S}_m^+$, alors (e_0, \dots, e_m) est une super-base M -obtus si et seulement si c'est une super-base et

$$\forall 0 \leq i, j \leq m, \langle e_i | M e_j \rangle \leq 0.$$

Grâce à une super-base M -obtus, on va pouvoir construire un M -maillage et c'est le résultat de la prochaine proposition.

Proposition 3.3. (*Construction d'un M -maillage*)

Soit $M \in \mathbb{S}_m^+$ et $(e_0, \dots, e_m) \in (\mathbb{Z}^m)^{m+1}$ une super-base M -obtus.

Pour construire $\mathcal{T}(M)$ on prend tous les simplexes qui ont pour sommets $\left(\sum_{i=0}^{k-1} e_{\sigma(i)} \right)_{0 \leq k \leq m}$ où $\sigma \in S_{m+1}$. Alors $\mathcal{T}(M)$ est un M -maillage

Démonstration. On va commencer par prouver les propriétés sur les simplexes. Soit (v_0, \dots, v_m)

les sommets d'un simplexe, ainsi il existe $\sigma \in S_{m+1}$ tel que pour $0 \leq k \leq m$, $v_k = \sum_{i=0}^{k-1} e_{\sigma(i)}$.

On a bien,

- $v_0 = 0$,
- $|\det(v_0, \dots, v_m)| = |\det(e_0, \dots, e_m)| = 1$,
- en remarquant que pour tout $1 \leq l, k \leq m$, $v_k = - \sum_{j=k}^m e_{\sigma(j)}$ (car $e_0 + \dots + e_m = 0$), on a donc

$$\langle v_l | M v_k \rangle = - \sum_{i=0}^{l-1} \sum_{j=k}^m \langle e_{\sigma(i)} | M e_{\sigma(j)} \rangle \geq 0,$$

car pour $0 \leq i, j \leq m$, $\langle e_i | M e_j \rangle \leq 0$.

Il nous reste à montrer que ce maillage couvre un voisinage de 0. La preuve complète se trouve dans l'article [6], nous ne la développerons pas ici, mais elle fait intervenir les simplexes de Khun et leur générateur de kernel. \square

Maintenant nous pouvons construire chaque voisinage à l'étape 1 de l'algorithme FM-LBR (2). Pour $x \in Z$ nous construisons \mathcal{T} un $\mathcal{M}(x)$ -maillage et nous posons

$$V(x) = x + \mathcal{T}. \quad (19)$$

Dans le cas où Z est décrit par (18), alors \mathcal{T} est un $R^T \mathcal{M}(x) R$ -maillage et de prendre pour voisinage

$$V(x) = x + hR\mathcal{T}.$$

La problématique devient donc la recherche des super-base M -obtus pour la construction des M -maillages, pour ça nous allons utiliser l'algorithme de réduction décrit par Phong Q. Nguyen et Damien Stehlé [6].

3.2.1 Construction d'une super-base M -obtus

Avant d'étudier les algorithmes, nous allons étudier comment on construit une super-base M -obtus, en partant d'une base M -réduite. Nous devons juste introduire une notation, pour $b_1, \dots, b_k \in \mathbb{R}^m$, nous noterons

$$b_1 \mathbb{Z} + \dots + b_k \mathbb{Z} = \{b_1 z_1 + \dots + b_k z_k; z_1, \dots, z_k \in \mathbb{Z}\},$$

et si $k = 0$ alors la somme vaut $\{0\}$ par convention. C'est simplement le réseau engendré par les vecteurs (b_1, \dots, b_d) .

Une grande partie de l'étude reposera sur les bases M -réduites, l'idée étant de trouver la base avec les vecteurs qui ont la plus petite norme possible.

Definition 3.5. (*Base M -réduite*)

Soient $1 \leq m \leq 4$, $M \in \mathbb{S}_m^+$ et (b_1, \dots, b_m) une base de \mathbb{Z}^m . (b_1, \dots, b_m) est une base M -réduite si et seulement si $|\det(b_1, \dots, b_m)| = 1$ et pour $1 \leq m \leq 4$,

$$b_k \in \operatorname{argmin} \{\|z\|_M; z \in \mathbb{Z}^m \setminus (b_1 \mathbb{Z} + \dots + b_k \mathbb{Z})\}.$$

L'idée derrière cette définition est de trouver les d vecteurs non colinéaires de plus petite norme. Dans la littérature, lorsque $M = I_m$ ces bases sont dites Minkowski réduite. Maintenant, l'objectif est de montrer les premières propriétés de ces bases pour pouvoir construire une super-base M -obtus.

Proposition 3.4. Soit $M \in \mathbb{S}_m^+$ et (b_1, \dots, b_m) une base M -réduite alors pour tout $1 \leq i \leq m$,

$$\|b_i\| \leq \kappa(M) \text{ et } \|b_i\|_M \leq \kappa(M) \|b_1\|_M \quad (20)$$

Et pour $z \in b_1 \mathbb{Z} + \dots + b_{i-1} \mathbb{Z} + b_{i+1} \mathbb{Z} + \dots + b_m \mathbb{Z}$ alors

$$2|\langle b_i | M z \rangle| \leq \|z\|_M^2. \quad (21)$$

Pour prouver ce résultat nous devons d'abord rappeler quelque résultats importants sur les matrices symétriques définies positives.

Proposition 3.5. Soit $M \in \mathbb{S}_m^+$, pour $x \in \mathbb{R}^m$, on a les résultats suivants :

1. $\|x\|_M \leq \|M\|^{1/2} \|x\|,$

$$2. \|M^{-1}x\|_M \leq \|M^{-1}\| \|x\|_M.$$

Démonstration. On sait que $M \in \mathbb{S}_m^+$, on peut donc noter les valeurs propres de M , $(\lambda_1, \dots, \lambda_m)$ et supposer que $0 < \lambda_1 \leq \dots \leq \lambda_m$. De plus on sait que $\|M\| = \lambda_m$, et d'après le théorème spectral il existe une base orthonormée de \mathbb{R}^d composée de vecteurs propres de M que l'on notera (e_1, \dots, e_m) .

Soit $x \in \mathbb{R}^m$, on peut écrire $x = \sum_{i=1}^m \mu_i e_i$, ainsi

$$\begin{aligned} \|x\|_M^2 &= \langle x | Mx \rangle \\ &= \sum_{i=1}^m \lambda_i \langle x | Me_i \rangle \quad \text{quitte à modifier l'ordre, on peut supposer que } Me_i = \lambda_i e_i \\ &\leq \lambda_m \langle x | x \rangle \\ &\leq \lambda_m \|x\|^2, \end{aligned}$$

or $\|M\| = \lambda_m$, on a donc prouvé le point 1.

De plus on sait que $M = OD^tO$ où B est la base canonique de \mathbb{R}^m , $O = \text{Mat}_B(e_1, \dots, e_m) \in \mathbb{O}_m(\mathbb{R})$ et $D = \text{diag}(\lambda_1, \dots, \lambda_m)$. On peut donc poser $\sqrt{D} = \text{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_m})$ et $\sqrt{M} = O\sqrt{D}^tO$ qui est donc une matrice symétrique et de plus $\sqrt{M}^2 = M$.

Ainsi $\|x\|_M = \|\sqrt{M}x\|$, on a donc,

$$\|M^{-1}x\|_M = \|M^{-1}\sqrt{M}x\| \leq \|M^{-1}\| \|\sqrt{M}x\| = \|M^{-1}\| \|x\|_M,$$

d'où le point 2. □

Passons à la preuve de la proposition 3.4.

Démonstration. On commence par montrer (20). Ainsi soit $i \in \llbracket 1 ; m \rrbracket$ et on note (e_1, \dots, e_m) la base canonique de \mathbb{Z}^m .

On sait qu'il existe $j \in \llbracket 1 ; m \rrbracket$ tel que $e_j \in b_1\mathbb{Z} + \dots + b_{i-1}\mathbb{Z}$ ainsi par la définition 3.5,

$$\|b_i\|_M \leq \|e_j\|_M \leq \|M\|^{1/2} \text{ par 1 car } \|e_j\| = 1.$$

Or

$$\begin{aligned} \|b_i\| &= \sqrt{\langle b_i | M^{-1}b_i \rangle_M} \\ &\leq \|b_i\|_M^{1/2} \|M^{-1}b_i\|_M^{1/2} && \text{en appliquant Cauchy-Schwarz} \\ &\leq \|b_i\|_M \|M^{-1}\|^{1/2}, && \text{en appliquant le point 2} \end{aligned}$$

ainsi $\|b_i\| \leq \kappa(M)$.

De plus comme $b_1 \in \text{argmin}\{\|z\|_M; z \in \mathbb{Z}^m \setminus \{0\}\}$, on a $\|b_1\| \geq 1$ donc $\|b_1\|_M \|M^{-1}\|^{1/2} \geq 1$ ainsi $\|b_1\|_M \kappa(M) \geq \|M\|^{1/2} \geq \|b_1\|_M$.

Pour (21), on fixe $z \in z \in b_1\mathbb{Z} + \dots + b_{i-1}\mathbb{Z} + b_{i+1}\mathbb{Z} + \dots + b_m\mathbb{Z}$ on a alors $b_i + z \notin b_1\mathbb{Z} + \dots + b_{i-1}\mathbb{Z}$ car (b_1, \dots, b_m) est une base. De plus par la définition 3.5 on a

$$\|b_i\|_M^2 \leq \|b_i + z\|_M^2 = \|b_i\|_M^2 + \|z\|_M^2 + 2\langle b_i | Mz \rangle,$$

donc $-2\langle b_i | Mz \rangle \leq \|z\|_M^2$. En faisant le même calcul avec $-z$ on obtient le résultat voulu. □

On peut maintenant construire une super-base M -obtus en dimensions 2 et 3 en partant d'une base M -réduite, c'est le but du prochain théorème.

Théorème 3.1. (Construction d'une super-base M -obtus)

Dimension 2 : Soit $M \in \mathbb{S}_2^+$ et (b_1, b_2) une base M -réduite. Alors si $\langle b_1 | Mb_2 \rangle \leq 0$ alors $(-b_1 - b_2, b_1, b_2)$ est une super-base M -obtus sinon $(b_1 - b_2, -b_1, b_2)$ est une super-base M -obtus.

Dimension 3 : Soit $M \in \mathbb{S}_3^+$ et (b_1, b_2, b_3) une base M -réduite. Si $\langle b_1 | Mb_2 \rangle \leq 0$ alors $(-b_1 - b_2 - b_3, b_1, b_2, b_3)$ est une super-base M -obtus sinon c'est $(-b_2 - b_3, -b_1, b_2, b_1 + b_3)$.

Démonstration. Dimension 2 : Quitte à multiplier b_1 par -1 , on peut supposer que $\langle b_1 | Mb_2 \rangle \leq 0$. On pose $(e_0, e_1, e_2) = (-b_1 - b_2, b_1, b_2)$ ainsi on a bien $e_0 + e_1 + e_2 = 0$, et par la définition d'une base M -réduite (définition 3.5) on sait que (e_1, e_2) est une base de \mathbb{Z}^2 et $|\det(e_1, e_2)| = 1$. De plus par (21) avec $i = 2$ et $z = b_1$, $2|\langle b_2 | Mb_1 \rangle| \leq \|b_1\|_M^2$ donc $-\langle b_1 | Mb_2 \rangle \leq \|b_1\|_M^2$, de même avec $i = 1$ et $z = b_2$, $2|\langle b_1 | Mb_2 \rangle| \leq \|b_2\|_M^2$ donc $-\langle b_1 | Mb_2 \rangle \leq \|b_2\|_M^2$. Ainsi

$$\langle e_1 | Me_0 \rangle = \langle b_1 | M - b_1 - b_2 \rangle = -\|b_1\|_M^2 - \langle b_1 | Mb_2 \rangle \leq 0$$

et

$$\langle e_2 | Me_0 \rangle = \langle b_2 | M - b_1 - b_2 \rangle = -\|b_2\|_M^2 - \langle b_1 | Mb_2 \rangle \leq 0.$$

Par ailleurs on sait que $\langle e_1 | Me_2 \rangle \leq 0$, ainsi (e_0, e_1, e_2) est une super-base M -obtus.

Dimension 3 : Permuter les vecteurs et/ou les multiplier par -1 cela ne change pas la valeur absolue du déterminant ni le fait que les vecteurs forment une base de \mathbb{Z}^3 . On peut donc supposer que

$$|\langle b_1 | Mb_2 \rangle| \leq \min \{ -\langle b_1 | Mb_3 \rangle, -\langle b_2 | Mb_3 \rangle \}. \quad (22)$$

Si $\langle b_1 | Mb_2 \rangle \leq 0$, alors on pose $(e_0, e_1, e_2, e_3) = (-b_1 - b_2 - b_3, b_1, b_2, b_3)$. On a bien $e_0 + e_1 + e_2 = 0$ et (e_1, e_2, e_3) est une base de \mathbb{Z}^3 avec $|\det(e_1, e_2, e_3)| = 1$.

De plus on sait par (22) que $\langle e_2 | Me_3 \rangle = \langle b_2 | Mb_3 \rangle \leq 0$, $\langle e_1 | Me_3 \rangle = \langle b_1 | Mb_3 \rangle \leq 0$ et

$$\begin{aligned} \langle Me_1 | e_0 \rangle &= \langle Mb_1 | -b_1 - b_2 - b_3 \rangle \\ &= -\|b_1\|_M^2 - \langle Mb_1 | b_2 \rangle - \langle Mb_1 | b_3 \rangle \\ &\leq -\|b_1\|_M^2 - 2\langle Mb_1 | b_3 \rangle && \text{car } -\langle Mb_1 | b_2 \rangle \leq -\langle Mb_1 | b_3 \rangle \text{ par (22)} \\ &\leq 0 && \text{car } 2|\langle b_3 | Mb_1 \rangle| \leq \|b_1\|_M^2 \text{ par (21) avec } i = 3 \text{ et } z = b_1. \end{aligned}$$

De même,

$$\begin{aligned} \langle Me_2 | e_0 \rangle &= \langle Mb_2 | -b_1 - b_2 - b_3 \rangle \\ &= -\|b_2\|_M^2 - \langle Mb_2 | b_1 \rangle - \langle Mb_2 | b_3 \rangle \\ &\leq -\|b_2\|_M^2 - 2\langle Mb_2 | b_3 \rangle && \text{car } -\langle Mb_2 | b_1 \rangle \leq -\langle Mb_2 | b_3 \rangle \text{ par (22)} \\ &\leq 0 && \text{car } 2|\langle b_3 | Mb_2 \rangle| \leq \|b_2\|_M^2 \text{ par (21) avec } i = 3 \text{ et } z = b_2. \end{aligned}$$

Et pour finir, dans le cas où $\langle Mb_3 | b_1 \rangle \leq \langle Mb_3 | b_2 \rangle$,

$$\begin{aligned} \langle Me_3 | e_0 \rangle &= \langle Mb_3 | -b_1 - b_2 - b_3 \rangle \\ &= -\|b_3\|_M^2 - \langle Mb_3 | b_1 \rangle - \langle Mb_3 | b_2 \rangle \\ &\leq -\|b_3\|_M^2 - 2\langle Mb_3 | b_2 \rangle \\ &\leq 0 && \text{car } 2|\langle b_2 | Mb_3 \rangle| \leq \|b_3\|_M^2 \text{ par (21) avec } i = 2 \text{ et } z = b_3. \end{aligned}$$

Le même raisonnement fonctionne si $\langle Mb_3 | b_1 \rangle > \langle Mb_3 | b_2 \rangle$ en utilisant (21) avec $i = 1$ et $z = b_3$.

Dans le cas où $\langle b_1 | Mb_2 \rangle > 0$, alors on pose $(e_0, e_1, e_2, e_3) = (-b_2 - b_3, -b_1, b_2, b_1 + b_3)$. On remarque

qu'en notant B la base canonique de \mathbb{Z}^3 on a $\text{Mat}_B(e_1, e_2, e_3) = \text{Mat}_B(b_1, b_2, b_3) \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Ainsi

(e_1, e_2, e_3) est une base de \mathbb{Z}^3 et $|\det(e_1, e_2, e_3)| = 1$.

Nous avons aussi

$$\begin{aligned} \langle -b_2 - b_3 | Mb_1 + b_3 \rangle &= -\|b_3\|_M^2 - \langle b_2 | Mb_1 \rangle - \langle b_3 | Mb_1 \rangle - \langle b_2 | Mb_3 \rangle \\ &\leq -\|b_3\|_M^2 - \langle b_3 | Mb_1 \rangle - \langle b_2 | Mb_3 \rangle && \text{car } \langle b_1 | Mb_2 \rangle > 0 \\ &\leq 0 \end{aligned}$$

On montre de la même manière, grâce à (21), que les autres produits scalaires sont négatifs. \square

Ainsi il nous reste juste à calculer numériquement les bases M -réduites en dimension 2 et 3. Pour ça nous allons utiliser les travaux de Phong Q. Nguyen et Damien Stehlé avec leur article [6] qui traite de la réduction des bases des réseaux en petite dimension.

Théorème 3.2. (Phong Q. Nguyen et Damien Stehlé [6])

Il existe un algorithme qui étant donné une matrice $M \in \mathbb{S}_m^+$ ($1 \leq m \leq 4$), renvoie une base M -réduite de \mathbb{Z}^m .

Dans la suite nous allons détailler l'algorithme en dimension 2 et celui en dimension 3 pour prouver ce résultat, en commençant par l'algorithme en dimension 2, l'algorithme de Lagrange.

3.2.2 Etude de l'algorithme de Lagrange

Lorsque l'on regarde la définition d'une base M -réduite, on se rend compte qu'en dimension 2 cela revient à trouver les deux plus petits vecteurs (pour la norme $\|\cdot\|_M$) du réseau qui sont non colinéaires. Pour ce faire cet algorithme peut-être vu comme une généralisation de l'algorithme d'Euclide mais en 2 dimensions.

Algorithm 3 Algorithme de Lagrange

Require: La base canonique (u, v) de \mathbb{Z}^2 et $M \in \mathbb{S}_2^+$

Ensure: Une base M -réduite.

- 1: $(u, v) \leftarrow (v, -u)$
 - 2: $v \leftarrow v - \left\lfloor \frac{\langle u|v \rangle_M}{\|u\|_M^2} \right\rfloor u$
 - 3: **while** $\|u\|_M > \|v\|_M$ **do**
 - 4: $(u, v) \leftarrow (v, -u)$
 - 5: $v \leftarrow v - \left\lfloor \frac{\langle u|v \rangle_M}{\|u\|_M^2} \right\rfloor u$
 - 6: **end while**
-

où pour $x \in \mathbb{R}$, $\lfloor x \rfloor$ correspond à l'entier le plus proche de x .

Pour étudier cet algorithme nous allons d'abord montrer une caractérisation des bases M -réduites en dimension 2.

Proposition 3.6. (Caractérisation en dimension 2)

Soit $M \in \mathbb{S}_2^+$ et (u, v) une base de \mathbb{Z}^2 telle que $|\det(u, v)| = 1$. (u, v) est une base M -réduite si et seulement si elle vérifie

$$\|u\|_M \leq \|v\|_M \text{ et } |\tau_M(v, u)| \leq \frac{1}{2} \text{ où } \tau_M(v, u) = \frac{\langle u|v \rangle_M}{\|u\|_M^2}. \quad (23)$$

Cette proposition nous explique pourquoi on cherche à approcher le projeté orthogonal de v sur u à chaque opération, le but étant de diminuer le défaut d'orthogonalité des 2 vecteurs tout en réduisant leur norme.

Pour la preuve de cette proposition nous allons montrer un lemme.

Lemme 1. Soit (u, v) une base vérifiant 23 alors en notant (u, v^*) la base orthogonalisée avec le principe de Gram-Schmidt on a la minoration :

$$\|v^*\|_M \geq \frac{\sqrt{3}}{2} \|v\|_M$$

Démonstration. On sait que $v = \tau_M(v, u)u + v^*$, de plus grâce à la condition 23 on a $\tau_M(v, u)^2 \|u\|_M^2 \leq \frac{\|v\|_M^2}{4}$. On en déduit,

$$\|v^*\|^2 = \|v\|_M^2 - \tau_M(v, u)^2 \|u\|_M^2 \geq \frac{3}{4} \|v\|_M^2$$

d'où $\|v^*\|_M \geq \frac{\sqrt{3}}{2} \|v\|_M$. □

On peut maintenant prouver la proposition 3.6.

Démonstration. \Rightarrow : Soit (u, v) une base M -réduite alors par la définition 3.5, $\|u\|_M \leq \|v\|_M$.

Raisonnons par l'absurde en supposant que $|\tau_M(v, u)| > \frac{1}{2}$ et posons $w = v - \lfloor \tau_M(v, u) \rfloor u$. Ainsi $w \neq v$ et $w \notin u\mathbb{Z}$, de plus on a

$$\|\tau_M(w, u)u\|_M = \|\tau_M(v, u)u - \lfloor \tau_M(v, u) \rfloor u\|_M \leq \frac{\|u\|_M}{2} < \tau_M(v, u)u.$$

Or les projections orthogonales de w et v sur $\langle u \rangle^\perp$ sont les mêmes ainsi $\|w\| < \|v\|$ ce qui contredit la définition 3.5.

\Leftarrow : Soit une base (u, v) vérifiant les conditions 23. Pour prouver que cette base est M -réduite il suffit de prendre $(x, y) \in \mathbb{Z}^2 \setminus (0, 0)$ et de montrer qu'en posant $w = xu + yv$ on a $\|w\|_M \geq \|v\|_M$ si $y \neq 0$ et $\|w\|_M \geq \|u\|_M$ sinon.

Cas 1 : $y = 0$.

Alors comme $x \in \mathbb{Z}^*$ on a $\|w\|_M \geq \|u\|_M$.

Cas 2 : $|y| \geq 2$.

On peut écrire $w = (x + y\tau_M(v, u))u + yv^*$ où (u, v^*) est la base orthogonalisée grâce au principe de Gram-Schmidt avec comme produit scalaire $\langle \cdot, \cdot \rangle_M$. On en déduit :

$$\begin{aligned} \|w\|_M^2 &\geq |y|^2 \|v^*\|_M^2 \\ &\geq 4 \frac{3}{4} \|v\|_M^2 \end{aligned} \quad \text{par le lemme 1 et car } |y| \geq 2$$

d'où $\|w\|_M \geq \|v\|_M$.

Cas 3 : $y = \pm 1$.

Comme $|\tau_M(v, u)| \leq \frac{1}{2}$ on en déduit $\langle u|v \rangle_M \geq -\frac{1}{2} \|u\|_M^2$. Ainsi

$$\begin{aligned} \|w\|_M^2 &= x^2 \|u\|_M^2 + 2xy \langle u|v \rangle_M + \|yv\|_M^2 \\ &\geq x^2 \|u\|_M^2 - |x| \|u\|_M^2 + \|v\|_M^2 && \text{car } \langle u|v \rangle_M \geq -\frac{1}{2} \|u\|_M^2 \text{ et } y = \pm 1 \\ &\geq \|v\|_M^2 && \text{car } x \in \mathbb{Z}. \end{aligned}$$

Ainsi (u, v) est bien une base M -réduite. □

On peut donc maintenant prouver que l'algorithme produit bien une base M -réduite.

Théorème 3.3. .

L'algorithme de Lagrange (3) calcule une base M -réduite avec une complexité en $\mathcal{O}(1 + \log_{\sqrt{3}}(\kappa(M)))$.

Démonstration. La base canonique avec laquelle l'algorithme commence sera notée (u_0, v_0) puis les vecteurs à partir de la ligne 2 (u_1, v_1) et (u_i, v_i) après $i - 1$ passages dans la boucle **while**. Nous allons commencer par montrer par récurrence que pour tout $i \in \mathbb{N}$, (u_i, v_i) est une base et $|\det(u_i, v_i)| = 1$.

Si $i = 0$ comme on part de la base canonique on a bien les résultats voulus et sinon pour $i \in \mathbb{N}$ on a

$$\text{Mat}_{(u_0, v_0)}(u_{i+1}, v_{i+1}) = \text{Mat}_{(u_0, v_0)}(u_i, v_i) \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & \lfloor \tau_M(u_i, v_i) \rfloor \end{pmatrix}}_{\in \text{GL}_2(\mathbb{Z})}.$$

Ainsi par récurrence (u_{i+1}, v_{i+1}) est une base de déterminant ± 1 .

En notant n le nombre total de passages dans la boucle on sait que $\|u_{n+1}\|_M \leq \|v_{n+1}\|_M$ et

$$\begin{aligned} |\tau_M(v_{n+1}, u_{n+1})| &= \left| \frac{\langle u_{n+1} | v_{n+1} \rangle_M}{\|u_{n+1}\|_M^2} \right| \\ &= \left| \lfloor \tau_M(u_n, v_n) \rfloor \frac{\|v_n\|_M^2}{\|v_n\|_M^2} - \frac{\langle v_n | u_n \rangle_M}{\|v_n\|_M^2} \right| && \text{car } v_{n+1} = \lfloor \tau_M(u_n, v_n) \rfloor v_n - u_n \\ &= |\lfloor \tau_M(u_n, v_n) \rfloor - \tau_M(u_n, v_n)| \\ &\leq \frac{1}{2}. \end{aligned}$$

Ainsi avec la proposition 3.6 on obtient que la base en sortie est M -réduite.

Maintenant, il nous reste à montrer que l'algorithme finit bien et de calculer sa complexité. Pour cela, nous devons étudier plus précisément ce que fait l'algorithme. On se place à l'étape 5 (on peut considérer que les étapes 1 et 2 ne sont qu'une étape en plus de la boucle), on note $x = \lfloor \tau_M(v, u) \rfloor = \left\lfloor \frac{\langle u | v \rangle_M}{\|u\|_M^2} \right\rfloor$ et on distingue plusieurs cas.

Cas $x = 0$:

Alors $\|v\|_M \geq \|u\|_M$ car à l'étape 4 on a échangé u et v , ainsi c'est la dernière opération et on sort de la boucle.

Cas $|x| = 1$:

- Si $\|v - xu\|_M \geq \|u\|_M$ c'est la dernière opération.
- Sinon comme $|x| = 1$, on a $\|u - xv\|_M < \|u\|_M$ c'est à dire que u peut-être "raccourci" avec v , or dans l'algorithme u est l'ancien vecteur v c'est donc possible si et seulement si on est à l'étape 2.

Cas $|x| \geq 2$:

On note comme précédemment v^* la composante orthogonale de v par rapport à u pour le produit scalaire $\langle \cdot | \cdot \rangle_M$, ainsi on peut écrire que $v = \tau_M(v, u)u + v^*$.

De plus comme $|x| = |\lfloor \tau_M(v, u) \rfloor| \geq 2$ on a $|\tau_M(v, u)| \geq 3/2$ ainsi,

$$\begin{aligned} \|v\|_M^2 &= \tau_M(v, u)^2 \|u\|_M^2 + \|v^*\|_M^2 \\ &\geq \frac{9}{4} \|u\|_M^2 + \|v^*\|_M^2, \end{aligned}$$

or

$$\begin{aligned} \|v - xu\|_M^2 &= \|(\tau_M(v, u) - x)u + v^*\|_M^2 \\ &= (\tau_M(v, u) - x)^2 \|u\|_M^2 + \|v^*\|_M^2 \\ &\leq \frac{1}{4} \|u\|_M^2 + \|v^*\|_M^2 && \text{car } x = \lfloor \tau_M(v, u) \rfloor. \end{aligned}$$

On en conclut,

$$\|v\|_M^2 \geq 2\|u\|_M^2 + \|v - xu\|_M^2.$$

Ainsi si $\|u\|_M \leq \|v - xu\|_M$ c'est la dernière itération, l'algorithme se termine sinon $\|u\|_M > \|v - xu\|_M$ c'est à dire,

$$\|v\|_M \geq \sqrt{3}\|v - xu\|_M.$$

Donc le produit des normes des deux vecteurs diminue d'un facteur $\sqrt{3}$ à chaque itération, sauf à la première ou à la dernière itération, ainsi comme il diminue strictement l'algorithme se termine. De plus on peut donc majorer le nombre de passages dans la boucle **while** par :

$$\mathcal{O}\left(1 + \log_{\sqrt{3}}(\max(\|u\|_M, \|v\|_M)) - \log_{\sqrt{3}}\left(\min_{w \in \mathbb{Z}^2 \setminus \{0\}} (\|w\|_M)\right)\right),$$

où (u, v) est la base canonique de \mathbb{Z}^2 .

Or dans la preuve de la proposition 3.4 on a montré que pour $w \in \operatorname{argmin}\{\|z\|_M; z \in \mathbb{Z}^m \setminus \{0\}\}$ on a $\|w\|_M \geq \|M^{-1}\|^{-\frac{1}{2}}$, c'est à dire $\min_{w \in \mathbb{Z}^2 \setminus \{0\}} (\|w\|_M) \geq \|M^{-1}\|^{-\frac{1}{2}}$.

De plus comme (u, v) est la base canonique on a la majoration $\max(\|u\|_M, \|v\|_M) \leq \|M\|^{\frac{1}{2}}$ d'après la proposition 3.5. Ainsi, dans notre configuration on peut majorer le nombre d'itérations par :

$$\mathcal{O}\left(1 + \log_{\sqrt{3}}(\kappa(M))\right).$$

On a donc prouvé la complexité voulue. □

Remarque 1. Cet algorithme est utilisé dans le cas général pour trouver la base minimale d'un réseau quelconque de dimension 2. Dans ce cas, on peut partir de n'importe quelle base du réseau avec M leur matrice de Gram. Une base minimale étant une base où les vecteurs sont les deux plus petits du réseau non colinéaires, d'où l'équivalence avec notre base M -réduite. C'est dans ce sens qu'il est étudié dans l'article de Phong Q. Nguyen et Damien Stehlé [6].

On peut donc maintenant passer à l'étude de l'algorithme en dimension 3.

3.2.3 Présentation de l'algorithme en dimension 3

Le but est de généraliser l'algorithme de Lagrange mais la difficulté est qu'ici pour approcher le projeté orthogonal il ne suffit pas d'arrondir à l'entier le plus proche chaque coefficient. Voici une version itérative de cet algorithme.

Algorithm 4 Base M -réduite en dimension 3 et 4

Require: $d \leq 4$, $M \in \mathbb{S}_d^+$ et la base canonique (b_1, \dots, b_d) de \mathbb{Z}^d ordonner par norme croissante.

Ensure: Une base M -réduite.

- 1: $k = 2$
 - 2: **while** $k \leq d$ **do**
 - 3: Calculer $c \in b_1\mathbb{Z} + \dots + b_{k-1}\mathbb{Z}$ le plus proche de b_k
 - 4: $b_k \leftarrow b_k - c$
 - 5: **while** $\|b_k\|_M \leq \|b_{k-1}\|_M$ **do**
 - 6: $(b_k, b_{k-1}) \leftarrow (b_{k-1}, b_k)$
 - 7: $k \leftarrow k - 1$
 - 8: **end while**
 - 9: $k \leftarrow k + 1$
 - 10: **end while**
-

Note : La boucle **while** à l'étape 5 sert simplement à ce que la base soit toujours ordonnée par norme croissante.

On peut remarquer que pour $d = 2$, on retrouve exactement l'algorithme de Lagrange, dans ce cas l'étape 3 se fait en approchant $\tau_M(b_1, b_2)$. La difficulté se trouve donc lorsqu'il faut trouver le vecteur le plus proche pour $d \geq 2$. L'idée est encore de partir du projeté orthogonal, puis faire une recherche en $\mathcal{O}(1)$ pour trouver le bon vecteur. On donne aussi une version récursive de cet algorithme, qui nous sera utile pour son étude.

Algorithm 5 Algorithme récursif

Require: $d \leq 4$, $M \in \mathbb{S}_d^+$ et la base canonique (b_1, \dots, b_d) de \mathbb{Z}^d ordonnée par norme croissante.

Ensure: Une base M -réduite.

```

1: if  $d = 1$  then
2:   return  $b_1$ 
3: else
4:   repeat
5:     Trier  $(b_1, \dots, b_d)$  par norme croissante,
6:     Appliquer l'algorithme à  $(b_1, \dots, b_{d-1})$ ,
7:     Calculer  $c \in b_1\mathbb{Z} + \dots + b_{d-1}\mathbb{Z}$  le plus proche de  $b_d$ ,
8:      $b_d \leftarrow b_d - c$ 
9:   until  $\|b_d\|_M \geq \|b_{d-1}\|_M$ 
10:  return  $(b_1, \dots, b_d)$ 
11: end if

```

3.2.4 Etude de l'algorithme en dimension 3 et 4

Commençons par expliquer comment on calcule le vecteur le plus proche. On se place dans le cas où on doit approcher t avec le réseau engendré par (b_1, \dots, b_{d-1}) , c'est à dire trouver $c \in b_1\mathbb{Z} + \dots + b_{d-1}\mathbb{Z}$ tel que $\|t - c\|_M = \min_{z \in b_1\mathbb{Z} + \dots + b_{d-1}\mathbb{Z}} \|t - z\|_M$.

On sait que si on s'intéresse à l'espace $\text{Vec}(b_1, \dots, b_{d-1})$, le vecteur que l'on cherche est $t^* := \sum_{i=0}^{d-1} y_i b_i$, le projeté orthogonal de t sur $\text{Vec}(b_1, \dots, b_{d-1})$ car on sait que $\|t - t^*\|_M = \min_{z \in \text{Vec}(b_1, \dots, b_{d-1})} \|t - z\|_M$.

Et donc

$$\forall z \in b_1\mathbb{Z} + \dots + b_{d-1}\mathbb{Z}, \|t - z\|_M^2 = \|t - t^*\|_M^2 + \|t^* - z\|_M^2.$$

Il nous faut donc minimiser $\|t^* - z\|_M$, c'est à dire que l'on a $t^* - c \in \text{Vor}_M(b_1, \dots, b_{d-1})$. Une première étape est donc de calculer les coordonnées de t^* et pour cela on peut remarquer que pour $i \in \llbracket 1 ; d-1 \rrbracket$, on a :

$$\langle t | b_i \rangle_M = \langle t^* | b_i \rangle_M = \sum_{j=1}^{d-1} y_j \langle b_j | b_i \rangle_M.$$

C'est à dire en notant $G = (\langle b_i | b_j \rangle_M)_{1 \leq i, j \leq d-1}$, la matrice de Gram de (b_1, \dots, b_{d-1}) par rapport au produit scalaire $\langle \cdot | \cdot \rangle_M$, on peut calculer efficacement (y_1, \dots, y_{d-1}) en utilisant :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_{d-1} \end{pmatrix} = G^{-1} \begin{pmatrix} \langle t | b_1 \rangle_M \\ \vdots \\ \langle t | b_{d-1} \rangle_M \end{pmatrix}.$$

En notant $c = \sum_{i=0}^{d-1} x_i b_i$, ici $(x_1, \dots, x_{d-1}) \in \mathbb{Z}^{d-1}$, on sait que $t^* - c \in \text{Vor}_M(b_1, \dots, b_{d-1})$. De plus en utilisant l'algorithme récursif 5 on voit que grâce à l'étape 6 (b_1, \dots, b_{d-1}) est déjà une base M -

réduite dès que $d > 2$ (ce point sera prouvé juste après), on peut donc utiliser le théorème 3.4 suivant. Nous ne démontrons pas ce théorème ici mais il est issue de l'article de B. N. Delone et N. N. Sandakova (voir [7]).

Théorème 3.4. (*Caractérisation des cellules de Voronoï*)

1. Soit (b_1, b_2) une base M -réduite soit $u \in \text{Vor}_M(b_1, b_2)$, en notant $u = xb_1 + yb_2$ on a : $|x| < \frac{3}{4}$ et $y \leq 2/3$.
2. Soit (b_1, b_2, b_3) une base M -réduite soit $u \in \text{Vor}_M(b_1, b_2, b_3)$, en notant $u = xb_1 + yb_2 + zb_3$ on a : $|x| < \frac{3}{2}$, $y \leq 4/3$ et $|z| \leq 1$.

Ainsi si $d = 3$ ou $d = 4$, il nous reste à lister tous les entiers possibles pour les coordonnées de c grâce au théorème 3.4 puis de trouver le vecteur le plus proche de t^* , ainsi cette recherche se fait en $\mathcal{O}(1)$. Et si $d = 2$ alors le vecteur le plus proche est simplement $c = \lfloor \tau_M(t, b_1) \rfloor b_1$, comme dans l'algorithme de Lagrange (3).

Si $d = 2$, l'algorithme se comportant comme celui de Lagrange (3) on a déjà prouvé (voir théorème 3.3) qu'il produisait bien une base M -réduite. Le but va être de prouver le même résultat pour $d = 3$ et $d = 4$, pour ça on commence par montrer cette propriété.

Proposition 3.7. *A la fin des algorithmes (5) et (4), (b_1, \dots, b_d) est une base ordonnée de \mathbb{Z}^d et pour $i \in \llbracket 2; d \rrbracket$ on a pour tout $x_1, \dots, x_{i-1} \in \mathbb{Z}$, $\|b_i\|_M \leq \|b_i + x_1 b_1 + \dots + x_{i-1} b_{i-1}\|_M$.*

Démonstration. La formulation "repeat ... until" dans la version récursive de l'algorithme 5, nous assure de faire les étapes de 5 à 9 au moins une fois. Ainsi on sait qu'en sortie de l'algorithme la famille (b_1, \dots, b_d) est ordonnée par norme croissante et c'est une base de \mathbb{Z}^d . Pour le montrer on note (b_1^0, \dots, b_d^0) la base canonique, (b_1^i, \dots, b_d^i) après le i -ème passage dans la boucle et $c_i := \sum_{j=0}^{d-1} y_j^i b_j$ le vecteur calculé à l'étape 7 lors du $i+1$ -ième passage dans la boucle. Ainsi il existe $\sigma \in S_d$ (grâce à l'étape 5) tel que

$$\text{Mat}_{(b_1^0, \dots, b_d^0)}(b_1^{i+1}, \dots, b_d^{i+1}) = \text{Mat}_{(b_1^0, \dots, b_d^0)}(b_{\sigma(1)}^i, \dots, b_{\sigma(d)}^i) \underbrace{\begin{pmatrix} 1 & & & -x_1 \\ & \ddots & & \vdots \\ & & 1 & -x_{i-1} \\ & & & 1 \end{pmatrix}}_{\in \text{GL}_d(\mathbb{Z})}.$$

Et donc, comme un part d'une base à la fin de l'algorithme, (b_1, \dots, b_d) est une base ordonnée de \mathbb{Z}^d .

De plus grâce au calcul de l'étape 7 on sait, qu'après l'étape 8, on a pour $i \in \llbracket 2; d \rrbracket$, $\|b_i\|_M = \min_{z \in b_1 \mathbb{Z} + \dots + b_{i-1} \mathbb{Z}} \|b_i - z\|_M$, d'où la propriété. \square

Il nous faut maintenant étudier plus précisément les base M -réduites. D'après leur définition, on pourrait penser que pour tester si une base est M -réduite, il faut tester une infinité de conditions. Or, un résultat important est que pour toute dimension il existe un nombre fini de conditions à tester pour vérifier qu'une base est M -réduite. Ce résultat est décrit par Carl Ludwig Siegel avec le "second finiteness theorem" dans son livre Lectures on the Geometry of Numbers [8]. Plus précisément, dans cet article [9] P. P. Tamela décrit les conditions à tester pour $d \leq 6$. Nous allons détailler dans le théorème suivant ces résultats pour $d \leq 4$.

Théorème 3.5. *On fixe $d \leq 4$ et $M \in \mathbb{S}_m^+$.*

(b_1, \dots, b_d) , une base ordonnée de \mathbb{Z}^d , est une base M -réduite si et seulement si pour tout $i \in \llbracket 1; d \rrbracket$ et pour tout uplet d'entiers x_1, \dots, x_d vérifiant les conditions 1 et 2 on a :

$$\|x_1 b_1 + \dots + x_d b_d\|_M \geq \|b_i\|_M.$$

1. $\text{pgcd}(x_1, \dots, x_d) = 1$,
2. il existe $\sigma \in S_d$ tel que $(|x_{\sigma(1)}|, \dots, |x_{\sigma(d)}|) \in C_d$ où

$$C_2 = \{(1, 1)\}$$

$$C_3 = \{(1, 1, 0), (1, 1, 1)\}$$

$$C_4 = \{(1, 1, 0, 0), (1, 1, 1, 0), (1, 1, 1, 1)\}$$

Nous ne détaillerons pas la preuve ici, elle repose sur l'étude des formes quadratiques mais elle se trouve dans [9]. Grâce à ce théorème, nous allons donc pouvoir démontrer que les algorithmes (5) et (4) trouvent une base M -réduite.

Théorème 3.6. *Pour $d \leq 4$.*

A la fin des algorithmes (5) et (4), (b_1, \dots, b_d) est une base M -réduite.

Démonstration. Grâce à la proposition 3.7, nous savons déjà qu'à la fin de l'algorithme (b_1, \dots, b_d) est une base ordonnée et pour $1 \leq i \leq d$

$$\forall x_1, \dots, x_{i-1} \in \mathbb{Z}^{i-1}, \|b_i\|_M \leq \|b_i + x_1 b_1 + \dots + x_{i-1} b_{i-1}\|_M. \quad (24)$$

Il nous reste à montrer que (b_1, \dots, b_d) vérifie les conditions données par le théorème 3.5. Nous allons détailler pour commencer le cas $d = 3$. Il nous faut pour cela montrer les inégalités suivantes :

$$\begin{aligned} \|b_3 \pm b_2 \pm b_1\|_M &\geq \|b_1\|_M & \|b_3 \pm b_1\|_M &\geq \|b_3\|_M \\ \|b_3 \pm b_2 \pm b_1\|_M &\geq \|b_2\|_M & \|b_3 \pm b_2\|_M &\geq \|b_3\|_M \\ \|b_3 \pm b_2 \pm b_1\|_M &\geq \|b_3\|_M & \|b_2 \pm b_1\|_M &\geq \|b_2\|_M \\ \|b_3 \pm b_2\|_M &\geq \|b_2\|_M. \end{aligned}$$

Tout d'abord on utilise (24) avec $i = 3$ et $(x_1, x_2) = (\pm 1, \pm 1)$, on a

$$\|b_3 \pm b_2 \pm b_1\|_M \geq \|b_3\|_M \geq \|b_2\|_M \geq \|b_1\|_M \text{ car } (b_1, b_2, b_3) \text{ est ordonnée.}$$

Puis en utilisant (24) avec $i = 3$, $(x_1, x_2) = (0, \pm 1)$ et $(x_1, x_2) = (\pm 1, 0)$, on a

$$\|b_3 \pm b_2\|_M \geq \|b_3\|_M \geq \|b_2\|_M \text{ et } \|b_3 \pm b_1\|_M \geq \|b_3\|_M$$

Et pour finir avec $i = 2$ et $x_1 = \pm 1$ on obtient la dernière inégalité $\|b_2 \pm b_1\|_M \geq \|b_2\|_M$.

La preuve dans le cas $d = 4$ est identique et elle fonctionne car dans les contions à tester on a que des 0 et des 1. \square

On peut se demander si pour $d \geq 5$ la base en sortie de l'algorithme 4 est toujours M -réduite. La réponse est non, on n'a plus l'équivalence entre les conditions montrées à la proposition 3.7 et le fait qu'une base soit M -réduite, un contre exemple est donné dans [6].

La dernière question que l'on doit se poser sur cet algorithme, c'est d'évaluer sa complexité et prouver qu'il se termine. Nous ne détaillerons pas cette partie ici, malgré son aspect assez simple son étude est assez complexe, elle est détaillée dans l'article [6]. Le résultat qui nous intéresse et que l'algorithme termine et que sa complexité temporelle est en

$$\mathcal{O} \left(1 + \log \left(\max_{i \in [1; d]} \|b_i\|_M \right) - \log \left(\min_{w \in \mathbb{Z}^d \setminus \{0\}} (\|w\|_M) \right) \right),$$

où (b_1, \dots, b_d) est la base canonique de \mathbb{Z}^d .

Comme pour le théorème 3.3 on peut réécrire cette complexité en fonction de la donnée qui nous intéresse c'est à dire la matrice M et on trouve une complexité temporelle en :

$$\mathcal{O} \left(1 + \log(\kappa(M)) \right).$$

On peut maintenant donc conclure sur la question qu'on se posait au début sur la construction d'un M -maillage dans notre algorithme. Pour cela, nous calculons tout d'abord une base M -réduite puis grâce au théorème 3.1 on peut construire une super-base M -obtus que nous utilisons pour construire un M -maillage avec la proposition 3.3. Ainsi en dimension le maillage aura cette forme :

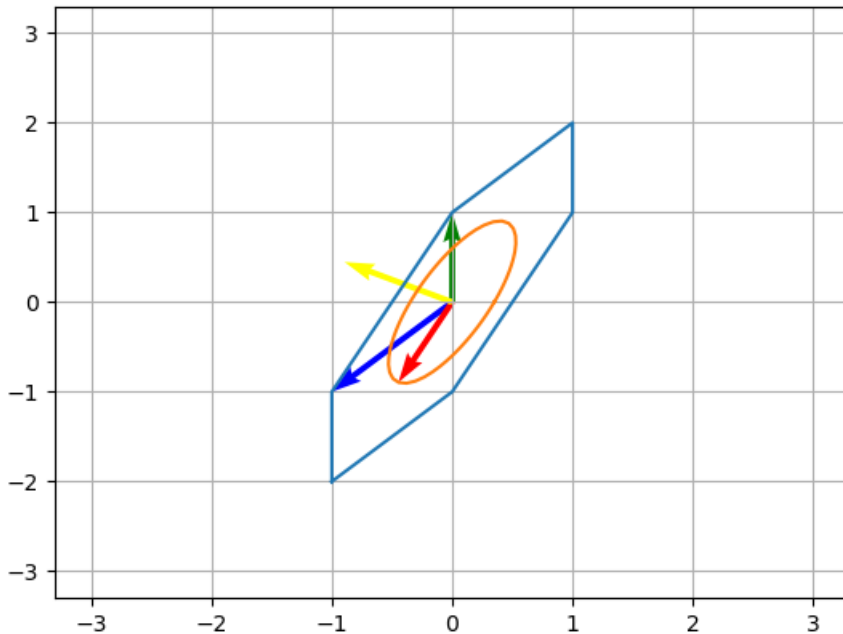


FIGURE 11 – Maillage en dimension 2 avec la base M -réduite.

En orange, on a la boule unité lié à $\|\cdot\|_M$, les vecteurs jaune et rouge sont les vecteurs propres de M (les valeurs propres étant 1 et 10), en bleu et vert on a la base M -réduite et en bleu le maillage calculé.

Pour différentes valeur propres et vecteurs propres on peut voir comment le maillage s'adapte, on garde le même code couleurs pour la signification des vecteurs :

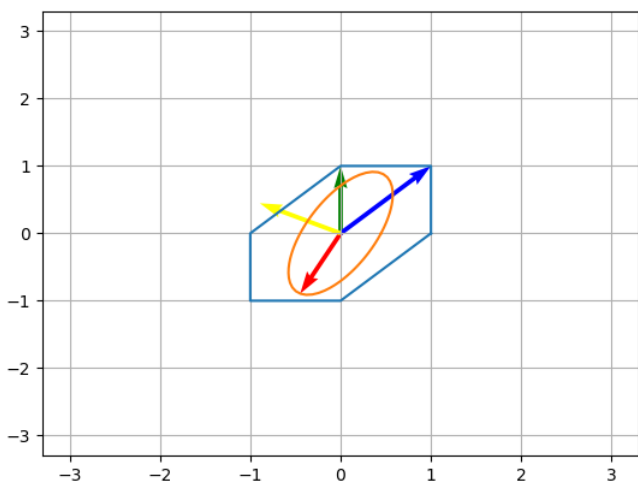


FIGURE 12 – Les valeurs propres de M sont 1 et 6.

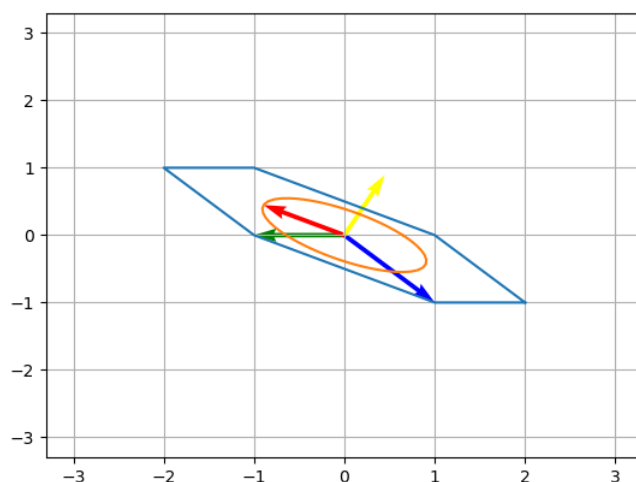


FIGURE 13 – On échange les deux vecteurs propres avec comme valeur propre 1 et 10

En dimension 3, le maillage s'oriente aussi dans la même direction que la boule unité, on peut le voir avec cette figure tirée de l'article [4] de Jean-Marie Mirebeau.

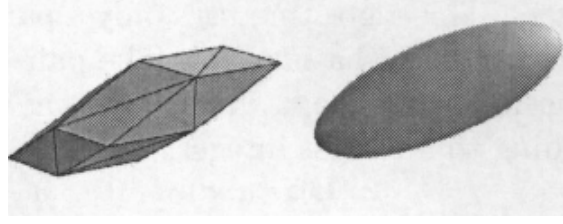


FIGURE 14 – Maillage en dimension 3, tiré de [4].

Maintenant qu'on a fini cette étude sur la construction du maillage, on va pouvoir approfondir les propriétés du M -maillage construit.

3.3 Etude de l'algorithme FM-LBR

On a pu détailler les propriétés pour un point fixé des M -maillages, mais pour que l'algorithme fonctionne le maillage que l'on construit doit vérifier des conditions plus strictes et c'est le but de la définition qui suit. Dans la suite, à chaque fois que nous parlerons d'un M -maillage nous désignerons un maillage construit comme nous l'avons détaillé précédemment.

Definition 3.6. (Maillage admissible)

$(\mathcal{T}(x))_{x \in \Omega}$ une famille de maillage est admissible s'il existe $r > 0$ et $R \in \mathbb{R}$ tels que pour tout $x \in \Omega$ on a :

1. $\mathcal{T}(x)$ couvre un voisinage de l'origine et les sommets appartiennent à \mathbb{Z}^m ,
2. pour tous sommets v de $\mathcal{T}(x)$, $\|e\| \leq R$,
3. il existe $B(x)$ une base de \mathbb{Z}^m telle que pour tout $z \in B(x)$ et pour tout $y \in \Omega$ tel que $\|x - y\| < r$ on a $z, -z \in \mathcal{T}(y)$.

Cette définition nous permet d'énoncer le théorème important de l'article [6], la preuve que la fonction en sortie de l'algorithme FM-LBR converge vers la solution de l'équation que l'on cherche (16).

Théorème 3.7. (Convergence de la solution)

Soit $\Omega \subset \mathbb{R}^m$ un ouvert borné, une métrique Riemannienne $\mathcal{M} \in C^0(\overline{\Omega}, \mathbb{S}_m^+)$ et la famille de maillage $(\mathcal{T}(x))_{x \in \Omega}$ que l'on a construit précédemment. Pour tout $h > 0$ on pose $Z_h = h\mathbb{Z}^m$ et pour tout $z \in Z_h \cap \Omega$ on considère le voisinage $V_h(z) = z + h\mathcal{T}(z)$.

Alors $(\mathcal{T}(x))_{x \in \Omega}$ est une famille de maillage admissible et la solution $d_h : Z_h \rightarrow \mathbb{R} \cup \{+\infty\}$ de l'équation discrète (17) converge uniformément vers la solution D de (16), ainsi :

$$\lim_{h \rightarrow 0} \max_{z \in Z_h \cap \Omega} |d_h(z) - D(z)| = 0.$$

Ainsi le but premier va être de montrer que le maillage que l'on construit respecte la définition 3.6, et c'est l'objectif de la proposition suivante.

Proposition 3.8. Soit $\mathcal{M} \in C^0(\overline{\Omega}, \mathbb{S}_m^+)$ une métrique riemannienne, alors la famille de maillage construit $(\mathcal{T}(x))_{x \in \Omega}$, en chaque point $\mathcal{T}(x)$ est un $\mathcal{M}(x)$ -maillage, est une famille de maillage admissible.

Le but va donc être de démontrer cette propriété, pour cela nous allons commencer à définir une nouvelle distance sur \mathbb{S}_m^+ .

Definition 3.7. (Définition distance sur \mathbb{S}_m^+)

Pour tout $M, N \in \mathbb{S}_m^+$ on définit :

$$\text{dist}(M, N) = \sup_{u \in \mathbb{R}^m \setminus \{0\}} |\ln \|u\|_M - \ln \|u\|_N| \quad (25)$$

Cette distance nous permet d'étudier le produit des normes d'un vecteur mesuré avec M et N alors que la distance classique, elle, permet d'étudier leur somme. On voit bien ce résultat avec le lemme suivant.

Lemme 2. Soit $M, N \in \mathbb{S}_m^+$, on pose $\alpha = \text{dist}(M, N)$ et $\beta = \|\sqrt{M} - \sqrt{N}\|$, où \sqrt{M} est définie dans la preuve de la propriété 3.5, on a pour tout $u \in \mathbb{R}^m$ tel que $\|u\| = 1$:

$$e^{-\alpha} \leq \frac{\|u\|_M}{\|u\|_N} \leq e^\alpha \text{ et } -\beta \leq \|u\|_M - \|u\|_N \leq \beta.$$

On en déduit pour tout $z \in \mathbb{R}^m$, $e^\alpha \|z\|_M \leq \|z\|_M \leq e^{-\alpha} \|z\|_M$.

Démonstration. Soit $u \in \mathbb{R}^m$ tel que $\|u\| = 1$.

Par (25), on sait que $\alpha = \text{dist}(M, N) \geq \ln \frac{\|u\|_M}{\|u\|_N}$, il suffit donc d'appliquer la fonction exponentielle. Pour la deuxième inégalité on utilise que :

$$\begin{aligned} |\|u\|_M - \|u\|_N| &= \left| \|\sqrt{M}u\| - \|\sqrt{N}u\| \right| \\ &\leq \left\| (\sqrt{M} - \sqrt{N})u \right\| \\ &\leq \left\| \sqrt{M} - \sqrt{N} \right\| = \beta \end{aligned} \quad \text{car } \|u\| = 1.$$

On a bien prouvé les deux encadrements. □

On va pouvoir, avec la proposition suivante, minorer la norme $\|\cdot\|_M$ d'un vecteur z du réseau qui ne fait pas partie du N -maillage que l'on a construit.

Proposition 3.9. Soit $M, N \in \mathbb{S}_m^+$.

Soit (u_1, \dots, u_m) une base M -réduite de \mathbb{Z}^m et \mathcal{T} un N -maillage. Soit $z \in \mathbb{Z}^m \setminus \mathcal{T}$ alors il existe un plus petit entier $l \in \llbracket 1 ; m \rrbracket$ tel que

$$z \in u_1 \mathbb{Z} + \dots + u_l \mathbb{Z} \text{ et } \|z\|_M^2 e^{4 \text{dist}(M, N)} \geq \|u_l\|_M^2 + \|u_1\|_M^2.$$

Démonstration. On notera comme dans le lemme 2, $\alpha = \text{dist}(M, N)$.

Tout d'abord on sait que \mathcal{T} couvre un voisinage de 0, donc il existe un simplexe T de \mathcal{T} , dont nous noterons les sommets non nuls (v_1, \dots, v_m) , et $\lambda > 0$ tel que λz appartient à l'intérieur du simplexe T . Comme on peut le voir pour la dimension 2 sur cette figure :

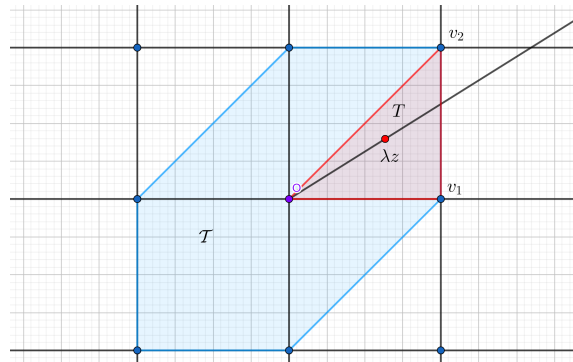


FIGURE 15 – Explication graphique

De plus on sait que (v_1, \dots, v_m) forme une base de \mathbb{Z}^m , ainsi il existe $\mu_1, \dots, \mu_m \in \mathbb{Z}$ tels que

$$z = \mu_1 v_1 + \dots + \mu_m v_m.$$

Plus précisément il existe $i, j \in \llbracket 1 ; m \rrbracket$ tels que $i \neq j$ et $\mu_i^2 \geq 1$ et $\mu_j^2 \geq 1$ où il existe $i \in \llbracket 1 ; m \rrbracket$ tel que $|\mu_i| \geq 2$, car z est non nul et n'appartient pas à \mathcal{T} . On en déduit que

$$\mu_1^2 + \dots + \mu_m^2 \geq 2$$

De plus, comme λz appartient à l'intérieur du simplexe T dont les sommets sont (v_1, \dots, v_m) , on peut supposer qu'il existe $1 \leq k \leq m$ tel que μ_1, \dots, μ_k soient strictement positifs et μ_{k+1}, \dots, μ_m nuls quitte à réorganiser (v_1, \dots, v_m) . On peut le voir en dimension 2 sur cette figure, la demi-droite $z\mathbb{R}^+$ est incluse dans $v_1\mathbb{R}^+ + \dots + v_m\mathbb{R}^+$:

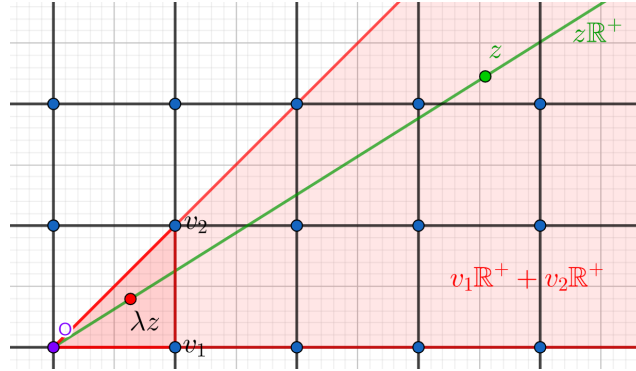


FIGURE 16 – Explication graphique

Comme $z \in \mathbb{Z}^m$ et que (u_1, \dots, u_m) est une base, il existe un plus petit entier $l \in \llbracket 1 ; m \rrbracket$ tel que $z \in u_1\mathbb{Z} + \dots + u_l\mathbb{Z}$. Il existe aussi $1 \leq j \leq k$ tel que $v_j \notin u_1\mathbb{Z} + \dots + u_{l-1}\mathbb{Z}$, sinon $z \in u_1\mathbb{Z} + \dots + u_{l-1}\mathbb{Z}$ ce qui contredit la définition de l .

En utilisant la définition d'une base M -réduite on a que $\|v_j\|_M \geq \|u_l\|_M$ et de même pour $i \in \llbracket 1 ; k \rrbracket$, v_i étant non nul on a $\|v_i\|_M \geq \|u_1\|_M$.

On peut donc prouver l'inégalité voulue,

$$\begin{aligned}
 e^{4\alpha} \|z\|_M^2 &\geq e^{2\alpha} \|z\|_N^2 && \text{par le lemme 2} \\
 &\geq e^{2\alpha} \left(\sum_{i=1}^k (\mu_i^2 \|v_i\|_N^2) + 2 \sum_{1 \leq i < \delta \leq k} (\mu_i \mu_\delta \langle v_i | v_\delta \rangle_N) \right) \\
 &\geq \sum_{i=1}^k (\mu_i^2 e^{2\alpha} \|v_i\|_N^2) && \text{car } \forall 1 \leq i < \delta \leq k, \mu_i \mu_\delta > 0 \text{ et } \langle v_i | v_\delta \rangle_N \geq 0 \\
 &\geq \sum_{i=1}^k (\mu_i^2 \|v_i\|_M^2) && \text{encore par le lemme 2} \\
 &\geq \sum_{\substack{i=1 \\ i \neq j}}^k (\mu_i^2 \|v_i\|_M^2) + (\mu_j^2 - 1) \|v_j\|_M^2 + \|v_j\|_M^2 \\
 &\geq \left(\sum_{i=1}^k (\mu_i^2) \right) \|u_1\|_M^2 + \|u_l\|_M^2 && \text{car } \forall 1 \leq i \leq k, \|v_i\|_M \geq \|u_1\|_M \text{ et } \|v_j\|_M \geq \|u_l\|_M \\
 &\geq \|u_l\|_M^2 + \|u_1\|_M^2 && \text{car } \mu_1^2 + \dots + \mu_k^2 \geq 2.
 \end{aligned}$$

La proposition est donc bien prouvée. □

Cette propriété va nous permettre de démontrer deux corollaires importants, on les utilisera pour prouver la proposition 3.8.

Corollaire 3.9.1. Soit $M, N \in \mathbb{S}_m^+$ tel que

$$\text{dist}(M, N) < \ln(1 + \kappa(M)^{-2})/4$$

alors en notant (b_1, \dots, b_m) une base M -réduite et \mathcal{T} un N -maillage on a que b_1, \dots, b_m et $-b_1, \dots, -b_m$ sont des sommets de \mathcal{T} .

Démonstration. Pour $1 \leq l \leq m$ alors $b_l \notin b_1\mathbb{Z} + \dots + b_{l-1}\mathbb{Z}$ mais $b_l \in b_1\mathbb{Z} + \dots + b_l\mathbb{Z}$. De plus en utilisant (20) de la proposition 3.4, on a

$$\|b_l\|_M^2 e^{4\text{dist}(M,N)} < \|b_l\|_M^2 + \kappa(M)^{-2} \|b_l\|_M^2 \leq \|b_1\|_M^2 + \|b_l\|_M^2.$$

Par contraposée de la proposition 3.9 on a que b_l est un sommet de \mathcal{T} , de même pour $-b_l$. \square

Corollaire 3.9.2. Soit $M \in \mathbb{S}_m^+$ avec $m \in \{2,3\}$.

Soit e un sommet de \mathcal{T} un M -maillage alors $\|e\| \leq C_m \kappa(M)$ où $C_2 = 2$ et $C_3 = 4$.

Démonstration. Soit (b_1, \dots, b_m) la base M -réduite avec laquelle on a construit \mathcal{T} . Ainsi d'après la construction que l'on a faite du maillage; pour e un sommet de \mathcal{T} il existe $\alpha_1, \dots, \alpha_m \in \mathbb{Z}$ tels que $e = \sum_{i=1}^m \alpha_i b_i$. En énumérant les possibilités, d'après la construction faite dans la proposition 3.3, on

a $\sum_{i=1}^m |\alpha_i| \leq C_m$ où $C_2 = 2$ et $C_3 = 4$.

De plus d'après (20) dans la proposition 3.4, on sait que $\max\{\|b_i\| \mid 1 \leq i \leq m\} \leq \kappa(M)$. On en déduit la majoration voulue. \square

Grâce à ces deux corollaires on va pouvoir maintenant passer à la preuve de la proposition 3.8.

Démonstration. On fixe $m \in \{2,3\}$, une métrique Riemmanienne $\mathcal{M} \in C^0(\overline{\Omega}, \mathbb{S}_m^+)$ et la famille de maillage $(\mathcal{T}(x))_{x \in \Omega}$ que l'on a construit où pour $x \in \Omega$, $\mathcal{T}(x)$ est un $\mathcal{M}(x)$ -maillage.

On doit montrer qu'il existe $r > 0$ et $R \in \mathbb{R}$ tel que pour tout $x \in \Omega$,

1. $\mathcal{T}(x)$ couvre un voisinage de l'origine et les sommets appartiennent à \mathbb{Z}^m ,
2. pour tout sommet v de $\mathcal{T}(x)$, $\|v\| \leq R$,
3. il existe $B(x)$ une base de \mathbb{Z}^m tel que pour tout $z \in B(x)$ et pour tout $y \in \Omega$ tel que $\|x - y\| < r$ on a $z, -z \in \mathcal{T}(y)$.

Tout d'abord, on sait que la fonction $\kappa \circ \mathcal{M} : \overline{\Omega} \leftarrow \mathbb{R}^+$ est continue sur un compact, on peut donc définir $\Delta(\mathcal{M}) = \sup_{x \in \overline{\Omega}} \kappa(\mathcal{M}(x)) \in \mathbb{R}$.

Plus précisément, grâce au théorème de Heine, on sait que \mathcal{M} est uniformément continue et par équivalence des normes sur \mathbb{S}_m^+ (dimension finie), il existe $r > 0$ tel que pour tout $y, w \in \overline{\Omega}$ tel que $\|w - y\| < r$ on a

$$\text{dist}(\mathcal{M}(w), \mathcal{M}(y)) \leq \ln(1 + \Delta(\mathcal{M})^{-2})/4.$$

Pour définir $R \in \mathbb{R}$, on pose simplement $R = C_m \Delta(\mathcal{M})$ où C_m est défini dans le corollaire 3.9.2. On peut maintenant fixer $x \in \Omega$ et montrer les points 1, 2 et 3.

Le point 1 a déjà été prouvé avec la proposition 3.3 lorsque qu'on explique comment on construit les maillages et le point 2, est une conséquence directe du corollaire 3.9.2.

Pour le point 3, on considère $(b_1(x), \dots, b_m(x))$ la base $\mathcal{M}(x)$ -réduite de \mathbb{Z}^m avec laquelle on a construit le maillage $\mathcal{T}(x)$. Soit $y \in \Omega$ tel que $\|x - y\| < r$ alors on a

$$\text{dist}(\mathcal{M}(w), \mathcal{M}(y)) \leq \ln(1 + \Delta(\mathcal{M})^{-2})/4 \leq \ln(1 + \kappa(\mathcal{M}(x))^{-2})/4.$$

Ainsi en utilisant le corollaire 3.9.1 on conclut que pour $i \in \llbracket 1 ; m \rrbracket$ on a $b_i(x) \in \mathcal{T}(y)$ et $-b_i(x) \in \mathcal{T}(y)$. \square

Nous avons maintenant quasiment tous les outils pour prouver le théorème 3.7. Nous ne pourrions détailler sa preuve complète ici, en effet c'est une légère adaptation de la preuve du théorème 11 de cette article [2] et elle demande beaucoup d'outils qui n'ont pas encore été abordé ici. Mais nous pouvons quand même démontrer une lemme important, ou l'objectif est de montrer une certaine régularité de la fonction $d_h : Z_h \longrightarrow \mathbb{R}$.

Lemme 3. On suppose les hypothèses du théorème 3.7.

Il existe une constante $h_0 > 0$ et $C_0 < +\infty$ tel que pour tout $0 < h \leq h_0$ et pour tout $x, y \in Z_h$, on a

$$\|d_h(x) - d_h(y)\| \leq C_0 \|x - y\| \quad (26)$$

Dans la preuve, nous utiliserons deux normes différentes sur \mathbb{R}^m , la norme $\|\cdot\|$ qui est celle liée au produit scalaire $\langle \cdot, \cdot \rangle$, que l'on utilise depuis le début et la norme 1, $\|\cdot\|_1$, qui est définie par

$$\left\| \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} \right\|_1 = \sum_{i=1}^m |\lambda_i|.$$

On note respectivement les normes $\|\cdot\|$ et $\|\cdot\|_1$ les normes d'opérateurs qu'elles engendrent sur $M_m(\mathbb{R})$. De plus on aura besoin de cette encadrement :

$$\forall x \in \mathbb{R}^m, \|x\| \leq \|x\|_1 \leq \sqrt{m} \|x\|.$$

Qui nous permet notamment de démontrer que :

$$\forall M \in M_m(\mathbb{R}), \|M\| \leq \sqrt{m} \|M\|_1.$$

Démonstration. Soient $h > 0$ et $x, y \in Z_h$, tout d'abord si $x \notin \Omega$ et $y \notin \Omega$ alors $d_h(x) = d_h(y) = 0$, l'inégalité est alors évidente.

Sinon, on peut supposer sans perte de généralité que $x \in \Omega$, on note $b(x) = (b_1(x), \dots, b_m(x))$ la base $\mathcal{M}(x)$ -réduite que l'on utilise pour construire $\mathcal{F}(x)$ le $\mathcal{M}(x)$ -maillage. Grâce à la proposition 3.8 on sait que pour $1 \leq i \leq m$, on a $\|b_i(x)\|_1 \leq R$.

En notant $e = (e_1, \dots, e_m)$ la base canonique de \mathbb{R}^m , on note $B = \text{Mat}_e(b(x))$. Par la définition 3.5 on sait que $|\det(B)| = 1$, car $B \in \text{GL}_m(\mathbb{Z})$. L'objectif va être de majorer la norme de B^{-1} . Pour ça on sait que $B^{-1} = \frac{1}{\det(B)} {}^t \text{Co}(B)$ or

$$\begin{aligned} \|{}^t \text{Co}(B)\|_1 &= \max_{1 \leq i \leq m} \sum_{1 \leq j \leq m} \Delta_{ij}(B) && \text{où } \Delta_{ij}(B) \text{ sont les mineurs de } B \\ &\leq \max_{1 \leq i \leq m} \sum_{1 \leq j \leq m} \|b_1^{(i)}\| \dots \|b_{j-1}^{(i)}\| \|b_{j+1}^{(i)}\| \dots \|b_m^{(i)}\| && \text{par le théorème d'Hadamard} \end{aligned}$$

où $b_k^{(i)}$ est le vecteur b_k sans la i -ième coordonnée lorsqu'il est écrit dans la base canonique. Ainsi $\|b_k^{(i)}\| \leq \|b_k^{(i)}\|_1 \leq \|b_k\|_1 \leq R$, on a donc

$$\|{}^t \text{Co}(B)\|_1 \leq mR^{m-1}$$

Ainsi $\|B^{-1}\| \leq \sqrt{m} \|B^{-1}\|_1 \leq m^{\frac{3}{2}} R^{m-1} := D_0$ car $|\det(B)| = 1$.

Dans un premier cas, on suppose que $\|x - y\|_1 = h$, comme $x, y \in \mathbb{Z}^m$ il existe $\varepsilon \in \{-1, 1\}$ et $1 \leq j \leq m$ tel que $y = x + \varepsilon h e_j$. En notant $B^{-1} = (\alpha_{kl})_{1 \leq k, l \leq m}$, on obtient

$$y = x + \varepsilon h \sum_{i=1}^d \alpha_{ij} b_i(x).$$

On peut donc définir $s = \sum_{i=1}^m |\alpha_{ij}| \in \mathbb{Z}$ et ainsi il existe une famille de vecteurs de \mathbb{Z}_h noté $(x_k)_{k=0}^s$ tel que $x_0 = x$, $y = x_s$ et pour $0 \leq k < s$ on a $x_{k+1} - x_k \in \{\pm h b_i(x) \mid 1 \leq i \leq m\}$. Ainsi pour $0 \leq k < s$, on a

$$\|x_{k+1} - x_k\| \leq h \max_{1 \leq i \leq m} \|b_i(x)\|_1 \leq hR.$$

Donc par l'inégalité triangulaire pour $0 \leq k \leq s$, $\|x_k - x\| \leq hRs$. Or par Cauchy-Schwartz on a,

$$s \leq \sqrt{m} \left(\sum_{i=1}^m \alpha_{ij}^2 \right)^{\frac{1}{2}} \leq \sqrt{m} \|B^{-1}\| \leq \sqrt{m} D_0.$$

Ainsi on peut conclure que pour $0 \leq k \leq s$, on a

$$\|x_k - x\| \leq \sqrt{m} h R D_0.$$

On peut maintenant définir $h_0 > 0$ telle que $\sqrt{m} h_0 R D_0 < r$, où r est celui utilisé dans le point 3 de la définition d'un maillage admissible, voir définition 3.6 (on peut l'utiliser grâce à la proposition 3.8). On peut donc fixer $0 < h \leq h_0$ et $0 \leq k \leq m$.

Si $x_k \in \omega$, alors on fixe $0 \leq l \leq s$ tel que $|k - l| = 1$. Par la définition de h_0 , on sait que $\|x_k - x\| \leq r$ ainsi en utilisant le point 3 de la définition 3.6, on a que pour tout $1 \leq i \leq m$, $b_i, -b_i \in \mathcal{F}(x_k)$. On en déduit que $x_l \in V_h(x_k)$ d'après (19), c'est à dire d'après la définition de l'opérateur de Hopf-Lax (voir (17)), on a :

$$d_h(x_k) = \Lambda(d_h, x_h) \leq \|x_k - x_l\|_{\mathcal{M}(x_k)} + d_h(x_l).$$

Or comme $\mathcal{M}(x_k) \in \mathbb{S}_m^+$, on a

$$\|x_k - x_l\|_{\mathcal{M}(x_k)} \leq \|\mathcal{M}(x_k)\|^{1/2} \|x_k - x_l\| \leq D_1 \|x_k - x_l\|_1 \leq h R D_1,$$

où $D_1 = \sup_{x \in \bar{\Omega}} \|\mathcal{M}(x)\|^{1/2}$ qui est fini par continuité de \mathcal{M} .

Sinon si $x \notin \Omega$ alors $d_h(x_k) = 0$ et donc $d_h(x_k) \leq d_h(x_l)$. En échangeant k et l , ce qui est possible car $\|x_l - x\| \leq r$, on obtient $|d_h(x_k) - d_h(x_l)| \leq h R D_1$. Par inégalité triangulaire on en déduit donc que

$$|d_h(x) - d_h(y)| \leq h R D_1 s \leq h \sqrt{m} R D_1 D_0 = \|x - y\|_1 C_0,$$

où $C_0 = R D_1 D_0 \in \mathbb{R}$.

Dans le cas où $\|x - y\|_1 > h$ alors il existe $n \in \mathbb{Z}$ tel que $\|x - y\|_1 = nh$ et il existe une famille de vecteurs de \mathbb{Z}_h notée $(x_k)_{k=0}^n$ tel que $x_0 = x$, $y = x_n$ et pour $0 \leq k < n$ on a $x_{k+1} - x_k \in \{\pm h e_i(x) \mid 1 \leq i \leq m\}$ donc $\|x_{k+1} - x_k\| = h$. Ainsi d'après le cas traité précédemment pour $0 \leq k < n$ on a $|d_h(x_{k+1}) - d_h(x_k)| \leq h C_0$, on peut donc utiliser l'inégalité triangulaire et on obtient :

$$|d_h(x) - d_h(y)| \leq n h c_0 = c_0 \|x - y\|_1.$$

Ainsi dans les deux cas traités en posant $C_1 = \sqrt{m} C_0$, on a le résultat voulu :

$$|d_h(x) - d_h(y)| \leq C_1 \|x - y\|$$

□

Ainsi nous avons démontré tous les points qui nous semblaient importants et accessibles sur l'algorithme FM-LBR. Pour voir la fin de la preuve du théorème 3.7, Jean-Marie Mirebeau, décrit dans [4], comment modifier la preuve du théorème 11 dans [2] pour obtenir le résultat voulu. Nous pouvons aussi donner la complexité complète de l'algorithme FM-LBR (2), la seule étape en plus par rapport à l'algorithme Fast-Marching (1) étant le calcul des voisinages pour chaque point, si on note $N = |Z|$ alors la complexité est en :

$$\mathcal{O}(N \log N + \log \Delta(\mathcal{M})).$$

De plus, Jean-Marie Mirebeau, dans son article [4], compare l'efficacité en pratique de cet algorithme par rapport à d'autres méthodes, il explique aussi comment cet algorithme peut-être utilisé pour calculer les géodésiques.

Références

- [1] G. Barles, “Solutions de viscosité et equations elliptiques du deuxième ordre.”
- [2] F. Bornemann and C. Rasch, “Finite-element discretization of static hamilton-jacobi equations based on a local variational principle,” Computing and Visualization in Science, vol. 9, 03 2004.
- [3] J.-M. Mirebeau, “Numerical schemes for anisotropic pdes on cartesian grid domains,” Numerical Analysis [math.NA]. Université Paris-Sud XI,, 2018.
- [4] J.-M. Mirebeau, “Anisotropic fast-marching on cartesian grids using lattice basis reduction,” SIAM Journal on Numerical Analysis , Vol. 52, No. 4 (2014), pp. 1573-1599.
- [5] G. Chenevier, “Théorie algébrique des nombres, cours de master 1 enseigné à l’École polytechnique 2011– 2019.”
- [6] D. S. Phong Q. Nguyen, “Low-dimensional lattice basis reduction revisited,” ACM Transactions on Algorithms, Association for Computing Machinery, 2009.
- [7] N. N. S. B. N. Delone, “Theory of stereohedra,” Trudy Mathematics Institute Steklov, 1961.
- [8] C. L. Siegel, Lectures on the Geometry of Numbers. Springer-Verlag, 1989.
- [9] P. P. Tammela, “On the reduction theory of positive quadratic forms.,” Soviet Mathematics Doklady, 1973.