Réduction de réseaux
Adaptations d'idées provenant du cas polynomial au cas entier.

HAI001I : Stage académique

Lucas Noirot
(lucas.noirot@etu.umontpellier.fr)

Encadrant
Romain Lebreton
(romain.lebreton@lirmm.fr)

17 février - 26 juin 2025

Remerciements

Table des matières

Liste des Algorithmes

Notations, complexité et acronymes

Cette section fait office de lexique et recense l'ensemble des notations et acronymes utilisées tout au long de ce mémoire.

Notations

$\mathbb{Z}$	L'ensemble des entiers relatifs.
$\mathbb{Q}$	L'ensemble des rationnels.
$\mathbb{R}$	L'ensemble des réels.
$\mathbb{K}$	Un corps quelconque.
$\mathbb{F}_p$	Un corps fini de caractéristique p.
$\mathbb{F}_p[x]$	L'anneau des polynômes univariés à coefficients dans le corps fini $\mathbb{F}_p$.
$\mathbb{F}_p^{\leq d}[x]$	Les polynômes à coefficients dans $\mathbb{F}_p$ de degré inférieur ou égal d.
$\mathbb{F}_p[x]^{m \times n}$	Les matrices $m \times n$ à coefficients dans $\mathbb{F}_p[x]$.
$\mathscr{L}$	Un réseau, désigné par une lettre majuscule calligraphiée.
$\mathscr{L}(B)$	Le réseau engendré par la matrice B.
B^T	La transposée de la matrice B.
B^*	La base de Gram-Schmidt associée à B.

Complexité

Multiplication dans $\mathbb{F}_p^{\leq d}[x]$	$\mathrm{M}(d) = \mathcal{O}(d \times \log d \times \log\log d)$.
Multiplication dans $\mathbb{F}_p^{n \times n}$	$\mathrm{MM}(n) = \mathcal{O}(n^\omega)$.
Multiplication dans $\mathbb{F}_p^{\leq d}[x]^{m \times n}$	$\mathrm{MM}(n,d) = \mathcal{O}(\mathrm{MM}(n)\,\mathrm{M}(d)) = \tilde{\mathcal{O}}(n^\omega d)$.

1

2

Acronymes

LLL	Lenstra–Lenstra–Lovász
SVP	Shortest Vector Problem
CVP	Closest Vector Problem

1. $\mathrm{MM}(n,d)$ peut également être obtenu via une approche d'évaluation-interpolation sur une suite géométrique, ce qui permet d'améliorer certaines bornes de complexité.
2. ω est l'exposant de la multiplication matricielle.

Guide de Lecture

DANS ce mémoire, chaque définition est suivie d'un exemple concret illustrant la notion en question, ainsi que d'un contre-exemple visant à en exposer les subtilités et exceptions éventuelles. Cette approche permet de mieux comprendre les conditions et les limitations associées à chaque concept. L'objectif est de clarifier les différences entre les situations avec lesquelles une définition est applicable et celles où elle ne l'est pas, afin de renforcer la compréhension approfondie des théorèmes et constructions présentés.

Introduction

Un réseau euclidien peut être intuitivement vu comme un ensemble discret et régulier de points dans l'espace $\mathbb{R}^n$, formant un sous-groupe discret additif. À titre d'exemple, dans le plan $\mathbb{R}^2$, un réseau correspond aux intersections d'un quadrillage régulier. Malgré leur ressemblance avec les espaces vectoriels classiques, les réseaux euclidiens possèdent des propriétés spécifiques et complexes, rendant invalides de nombreux résultats habituellement vérifiés dans les $\mathbb{K}$-espaces vectoriels. Cette complexité fait des réseaux euclidiens un objet d'étude particulièrement riche à la frontière de plusieurs domaines de mathématiques et d'informatiques, en particulier la cryptographie.

Un des problèmes fondamentaux liés aux réseaux euclidiens est la réduction de réseaux, qui consiste à déterminer une "bonne" base, c'est-à-dire une base qui facilite la résolution efficace de divers problèmes algorithmiques comme celui du vecteur le plus court ou du vecteur le plus proche d'une cible donnée. Ces deux problèmes sont connus pour être NP-complets et constituent précisément la difficulté à la base des cryptosystèmes reposant sur les réseaux euclidiens. Tandis que ces questions apparaissent simples et intuitives en basse dimension, elles deviennent rapidement très complexes et coûteuses à résoudre en grande dimension.

Pour mieux comprendre ces difficultés intrinsèques, il est pertinent d'étudier les réseaux polynomiaux, une classe analogue aux réseaux euclidiens mais algorithmiquement plus abordable. Alors que les réseaux euclidiens posent des problèmes NP-difficiles, les réseaux polynomiaux peuvent être réduits exactement et efficacement en temps polynomial. Cette différence fondamentale ouvre une piste prometteuse : serait-il possible d'adapter certaines méthodes exactes de réduction, initialement développées pour les réseaux polynomiaux, au cas des réseaux entiers ?

L'objectif précis de ce stage est donc d'explorer et de comparer les réseaux euclidiens et polynomiaux, et plus particulièrement d'analyser la possibilité d'adapter les techniques exactes issues des réseaux polynomiaux au contexte des réseaux entiers. Cette étude vise à évaluer l'efficacité potentielle de telles adaptations, à identifier les obstacles théoriques ou pratiques à surmonter, et à mieux comprendre les implications sur la sécurité cryptographique.

La pertinence cryptographique de cette démarche s'inscrit dans un contexte où les systèmes de sécurité actuels, reposant sur la difficulté de la factorisation des grands nombres premiers et du calcul de logarithmes discrets, risquent d'être mis à mal par les progrès en informatique quantique. À l'opposé, les réseaux euclidiens apparaissent comme une alternative prometteuse en cryptographie post-quantique, plusieurs de leurs problèmes fondamentaux semblant résister efficacement aux attaques quantiques. Un exemple emblématique de l'ambivalence algorithmique des réseaux euclidiens est l'algorithme LLL (Lenstra-Lenstra-Lovász), initialement célèbre pour avoir permis la cryptanalyse de systèmes basés sur le problème du sac à dos, mais qui joue aujourd'hui paradoxalement un rôle clé dans la conception de nouveaux schémas cryptographiques robustes. Ainsi, approfondir la compréhension et améliorer les techniques de réduction de réseaux euclidiens représente un enjeu crucial pour le développement futur de la cryptographie sécurisée face aux défis quantiques.

CHAPITRE 1

Réseaux euclidiens et polynomiaux

L'ÉTUDE des réseaux euclidiens puise ses racines dans les travaux mathématiques du XVIII^{e} siècle, notamment ceux de Leonhard Euler sur l'organisation géométrique des points dans l'espace. C'est cependant en 1891 qu'Hermann Minkowski établit véritablement les fondements modernes avec l'introduction de la théorie géométrique des nombres, reliant explicitement les réseaux à divers problèmes d'optimisation et de minimisation. Ses résultats joueront ultérieurement un rôle déterminant dans le développement de la cryptographie moderne. Néanmoins, c'est au cours du XX^{e} siècle, et plus particulièrement à partir des années 1990, que les réseaux euclidiens connaissent une véritable intégration dans la cryptographie. Les travaux de chercheurs tels que Ajtai, Dwork ou Regev marquent alors un tournant décisif, en démontrant que les difficultés algorithmiques intrinsèques aux réseaux peuvent constituer une base solide pour la conception de nouveaux systèmes cryptographiques résistants aux attaques conventionnelles et quantiques. Ce chapitre vise précisément à introduire de manière approfondie les concepts fondamentaux liés aux réseaux euclidiens, ainsi qu'à explorer les réseaux polynomiaux, leurs propriétés spécifiques et leurs liens avec les réseaux euclidiens.

1.1 Réseaux euclidien

1.1.1 Définitions et exemples

Nous considérons un espace euclidien, c'est-à-dire un espace vectoriel réel de dimension finie muni d'un produit scalaire, noté $\langle f, g \rangle$. Dans ce chapitre, nous utiliserons le produit scalaire usuel défini par $\langle f, g \rangle := f \cdot g^t = \sum_{i=1}^{n} f_i g_i$, lequel induit la norme-2 donnée par $\|f\|_2 = \sqrt{\sum_{i=1}^{n} f_i^2}$. Pour alléger les notations, nous omettrons souvent l'indice 2. Ce chapitre se contentera d'exposer les résultats classiques, sans chercher à en fournir de démonstration. Rappelons qu'au sein de $\mathbb{R}^n$, toutes les normes sont équivalentes, ce qui signifie qu'aucune ne change la nature intrinsèque des problèmes que nous aborderons. [1] Nous nous concentrerons néanmoins sur la norme-2 pour sa simplicité géométrique, car elle offre une mesure intuitive des longueurs et des angles, point essentiel pour étudier la structure des réseaux euclidiens. Afin de simplifier l'écriture, nous désignerons par $\mathcal{B} = (b_1, \ldots, b_n)$ une base de $\mathbb{R}^n$ et par $\mathcal{B}^* = (b_1^*, \ldots, b_n^*)$ sa base orthogonalisée par le procédé de Gram-Schmidt. Les matrices B et B^* (sans calligraphie) seront respectivement les matrices dont les lignes sont $b_1, \ldots, b_n$ et $b_1^*, \ldots, b_n^*$. Ces différentes écritures faciliteront la manipulation des vecteurs et la comparaison des longueurs dans la suite.

Plusieurs définitions équivalentes d'un réseau euclidien coexistent dans la littérature, selon que l'on se place ou non dans un espace euclidien $\mathbb{R}^n$, ou dans un espace $\mathbb{R}^n$ équipé explicitement d'une forme quadratique définie positive. Dans tous les cas, l'idée générale reste la même : un réseau euclidien est un sous-ensemble discret de $\mathbb{R}^n$ formé par toutes les combinaisons linéaires entières d'un ensemble de vecteurs générateurs.

1. En dimension fixée, résoudre **exactement** le problème **SVP** pour la norme $\|\cdot\|_\infty$ fournit en fait une γ-approximation (avec γ dépendant de la dimension) pour le problème **SVP** dans la norme $\|\cdot\|_2$. Il existe notamment une constante C telle que $\|v\|_2 \leq C\|v\|_\infty$ pour tout $v \in \mathbb{R}^n$. Ainsi, un vecteur minimisant $\|v\|_\infty$ donne un vecteur $\sqrt{n}$-proche du vecteur réellement le plus court en norme euclidienne.

Définition 1.1. Soit $n \in \mathbb{N}^*$, $b_1, \ldots, b_n \in \mathbb{R}^n$. Les définitions suivantes sont équivalentes.

- $\bigoplus_{1 \leq i \leq n} \mathbb{Z}b_i := \{a_1 b_1 + \cdots a_n b_n : a_i \in \mathbb{Z}\}$ est un **réseau euclidien.**
- Un **réseau euclidien** est un sous-groupe discret de $\mathbb{R}^n$.
- Un **réseau euclidien** est un $\mathbb{Z}$-module libre de type fini de $\mathbb{R}^n$.

Il existe une famille $\mathbb{Z}$-libre maximale $(b_i)_{1 \leq i \leq m}$ dans $\mathscr{L}$ tel que $\mathscr{L} = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_m$, est appelée **base** de $\mathscr{L}$, si on note B la matrice de la famille $(b_i)_{1 \leq i \leq m}$ on notera $\mathscr{L}(B)$ le réseau de base B, donc engendré par la famille $(b_i)_{1 \leq i \leq m}$.
L'entier m est commun à toutes les bases de $\mathscr{L}$ et on l'appelle **rang** de $\mathscr{L}$. Lorsque $n = m$, on dit que le réseau est de **rang plein**.

Exemple. Les entiers de Gauss, définit par $\mathbb{Z}[i] := \mathbb{Z} \oplus i\mathbb{Z}$ forment un réseau de rang 2 dans $\mathbb{C}$, c'est même un anneau.

Exemple. Un exemple plus exotique, $\mathbb{Z} \oplus \sqrt{2} \cdot \mathbb{Z}$ est un réseau de rang 2 dans $\mathbb{R}$.

Contre exemple. $\mathbb{Q}$ n'est pas un réseau euclidien , car $\mathbb{Q}$ est dense dans $\mathbb{R}$, ce qui brise la discrétude, bien que ce soit un sous-groupe de $\mathbb{R}$.

Proposition 1.1. Soit $\mathscr{L}$ et $\mathscr{L}'$ deux réseaux de rang n de base B et B'. Alors $\mathscr{L} = \mathscr{L}'$ si et seulement si il existe $U \in GL_n(\mathbb{Z})$ tel que $B' = BU$.

Toutes les bases d'un réseau euclidien diffèrent d'une transformation de déterminant ± 1. L'ensemble de ces transformations est connu sous le nom de groupe unimodulaire.

Remarque. On a l'action de groupe

$$\begin{aligned} \mathrm{GL}_n(\mathbb{Z}) \times \mathrm{GL}_n(\mathbb{R}) &\longrightarrow \mathrm{GL}_n(\mathbb{R}) \\ (U, \mathbf{B}) &\longmapsto \mathbf{B}U \end{aligned}$$

Un réseau est exactement une orbite de cette action. La réduction de réseaux consiste à trouver un bon représentant pour chaque orbite.

Existe-t-il une notion de bonne base dans les réseaux euclidiens ? Nous verrons qu'une base idéale est celle qui est la plus orthogonale possible. Il n'existe pas toujours de base strictement orthogonale, ce qui justifie la notion de quasi orthogonalité. Nous allons rajouter des façons de mesurer la qualité d'une base.

Remarque. Nous avons la suite d'inclusions suivante : $2\mathbb{Z} \subset \mathbb{Z} \subset \frac{1}{2}\mathbb{Z}$. On observe que $\mathrm{rang}(2\mathbb{Z}) = \mathrm{rang}(\mathbb{Z}) = \mathrm{rang}(\frac{1}{2}\mathbb{Z})$, bien que ces ensembles soient distincts, c'est-à-dire $2\mathbb{Z} \neq \mathbb{Z} \neq \frac{1}{2}\mathbb{Z}$. Ce phénomène montre que, contrairement aux espaces vectoriels, pour les réseaux, avoir une relation d'inclusion et avoir le même rang ne suffit pas à garantir l'égalité.

Nous présentons maintenant deux **invariants** fondamentaux d'un réseau :

— La **taille du vecteur minimal** du réseau, notée $\lambda_1(\mathscr{L})$,
— Le **volume du réseau**, aussi appelé la **taille du réseau** souvent désigné par $|\mathscr{L}|$.

Définition 1.2. Un **sous-réseau** $\mathscr{L}'$ de $\mathscr{L}$ est un sous groupe de $\mathscr{L}$, on notera $\mathscr{L}' \subseteq \mathscr{L}$.

Définition 1.3. La **taille**[2] d'un réseau $\mathscr{L}(B)$ est $\det(B)$ et est noté $|\mathscr{L}|$. La taille d'un réseau est

2. "taille" et "volume" sont synonymes, mais l'usage le plus courant dans la littérature anglaise est "déterminant du

indépendante de la base choisie.

Remarque. On peut définir de façon équivalente $|\mathscr{L}| := \sqrt{\det(\text{Gram(B)})}$ où $\text{Gram}(B) = B^t \cdot B$. On peut voir $|\mathscr{L}|$ comme le **volume du domaine fondamental** de $\left\{ \sum_{i=0}^{n} \lambda_i b_i \mid 0 \leq \lambda_i < 1 \right\}$.

Proposition 1.2. Soit $\mathscr{L}$, $\mathscr{L}'$ deux réseaux de $\mathbb{R}^n$ tel que $\mathscr{L}' \subseteq \mathscr{L}$ alors $\frac{|\mathscr{L}'|}{|\mathscr{L}|} \in \mathbb{N}$.

Remarque. Ce résultat est une conséquence directe du théorème de Lagrange.

Remarque. On remarque également qu'un ensemble de points non alignés dans un réseau ne constitue pas nécessairement une base si son déterminant est différent de $\pm|\mathscr{L}|$.

Définition 1.4. On appelle **minimum d'un réseau**[3] $\mathscr{L}$ la quantité

$$\lambda_1(\mathscr{L}) = \min_{\substack{v \in \\ v \neq 0}} \|v\|$$

Plus généralement, pour $k \in \{1, \ldots, n\}$, on pose $\lambda_k(\mathscr{L})$ le plus petit réel r tel qu'il existe k vecteurs $\mathbb{R}$-linéairement indépendants dans $\mathscr{L}$ de norme au plus r.

Remarque. $\lambda_1(\mathscr{L})$ correspond à la distance minimale dans un réseau. On peut y voir une analogie avec les codes linéaires.

Exemple. Les bases $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $B' = \begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$ engendrent le même réseau.
Ici $U = B'^{-1} = \begin{pmatrix} -1 & -1 \\ -2 & -1 \end{pmatrix}$ et $\det(U) = -1$. Donc B et B' engendrent le même réseau $\mathscr{L}$. On a $|\mathscr{L}| = 1$ et $\lambda_1(\mathscr{L}) = \lambda_2(\mathscr{L}) = 1$. On voit dans cet exemple que différentes bases peuvent être associées à un même réseau.

Théorème 1.1 (Premier théorème de Minkowski)**.** Pour tout $n \in \mathbb{N}^*$, il existe une constante $C_n > 0$ telle que pour tout réseau $\mathscr{L}$ de $\mathbb{R}^n$, on a :

$$\lambda_1(\mathscr{L}) \leq C_n |\mathscr{L}|^{1/n}$$

On peut prendre cette constante égale à $C_n = (2/\sqrt{\pi})\Gamma(n/2+1)^{1/n}$. On appelle **constante de Hermite-Minkowski** le carré de la constante optimale possible pour cette inégalité, noté γ_n, en particulier, on a $\gamma_n \leq C_n$.

Remarque. Comme $|\mathscr{L}|$ est un invariant du réseau, si on a n'importe quelle base du réseau , on peut trouver une approximation de λ_1.

Exemple. Le **réseau hexagonal**, ou **réseau en nid d'abeille**, est un réseau euclidien de $\mathbb{R}^2$ de rang 2, et est donné par la base $B = \begin{pmatrix} 1 & \frac{1+\sqrt{3}}{2} \\ 1 & \frac{1-\sqrt{3}}{2} \end{pmatrix}$. On a $\text{Gram}(B) = B^t B = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. On a $|\mathscr{L}| = \sqrt{3}$, et $\lambda_1 = \sqrt{2}$, donc $\gamma(L) = \frac{2}{\sqrt{3}}$. Ce réseau a la propriété de contenir des hexagones réguliers. En traçant des sphères de centre les points et de rayon $\sqrt{2}$, on obtient un empilement compact le plus dense en dimension 2.

réseau" ou "volume".

3. on peut aussi le définir comme $\lambda_1(\mathscr{L}) = \min\{r > 0 : |\mathcal{B}(r) \cap \mathscr{L}| > 1\} \in \mathbb{R}_+$

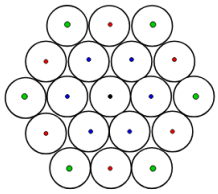

FIGURE 1.1 – Empilement hexagonal dans $\mathbb{R}^2$

Théorème 1.2. Soit $\mathscr{L}$ un réseau de $\mathbb{R}^n$. Soit S une partie convexe symétrique de $\mathbb{R}^n$ telle que $vol(S) > 2^n|\mathscr{L}|$, alors il existe $s \in \mathscr{L} \cap S$ non nul. De plus, cette inégalité est large si on suppose S compact.

Théorème 1.3 (Inégalité d'Hadamard)**.** Soit $B \in M_n(\mathbb{K})$. On a $|\det(B)| \leq \prod_{i=1}^{n} \|b_i\|$. La borne est atteinte si, et seulement si $(b_i)_{1\leq i\leq n}$ est une famille orthogonale.

Corollaire 1.1. Soit $\mathscr{L}$ un réseau de base B alors $|\mathscr{L}| = |\det(B)| \leq \prod_{i=1}^{n} \|b_i\|$.

Il existe un lien intéressant entre la base de Gram-Schmidt associée à une base de réseau et la norme du plus court vecteur de ce réseau. Le lecteur pourra se référer à l'annexe dédiée pour un rappel sur le procédé de Gram-Schmidt.

Proposition 1.3. Soit $\mathscr{L} \subset \mathbb{R}^n$ un réseau de base $b_1, \ldots, b_n$ et soit $b_1^*, \ldots, b_n^*$ sa base de Gram-Schmidt associée.
Alors pour tout $x \in \mathscr{L}\backslash\{0\}$, on a $\|x\| \geq \min\{\|b_1^*\|, \ldots, \|b_n^*\|\}$. En particulier, $\lambda_1(\mathscr{L}) \geq \min\{\|b_1^*\|, \ldots, \|b_n^*\|\}$.

1.1.2 Quelques problèmes algorithmiques liés aux réseaux euclidiens

Le calcul du plus court vecteur dans un réseau euclidien de $\mathbb{R}^n$ est un problème difficile. Qui sert de fondation à de nombreuses primitives cryptographiques. Considérons le problème suivant, paramétré par le rang n du réseau :

— **Shortest Vector Problem (SVP)** : Étant donné une base B d'un réseau $\mathscr{L}$, trouver un vecteur $v \neq 0$ tel que $\|v\| = \lambda_1(\mathscr{L})$. Ce problème est **NP-complet**, AJTAI 1996.

On ne connaît que des algorithmes demandant au moins un nombre exponentiel d'opérations pour résoudre ce problème, même en utilisant des algorithmes quantiques. Il y a deux types d'algorithmes qui se démarquent pour ce problème :

— **Les algorithmes de type énumération** : ils énumèrent tous les vecteurs du réseau qui sont dans une certaine boule bien choisie, en pratique ils sont utilisés jusqu'aux dimensions $n \approx 80$. On peut leur ajouter des optimisations et des heuristiques.
— **Les algorithmes de type crible** : on génère deux listes d'éléments du réseau, puis on construit la liste de toutes les différences entre les éléments des deux listes. On espère obtenir des vecteurs plus court. On recommence le procédé. Le temps d'exécution est en $2^{\mathcal{O}(n)}$.

On s'intéresse souvent à une version approximative plus accessible :

— **SVP**$_\gamma$, où $\gamma > 0$: Étant donné une base B du réseau $\mathscr{L}$, trouver un vecteur $v \neq 0$ tel que $\|v\| \leq \gamma \cdot \lambda_1(\mathscr{L})$.

L'état des connaissances actuelles est le suivant :

— Pour $\gamma = \mathcal{O}(1)$, le problème est prouvé **NP-complet**.
— Pour $\gamma = \text{poly}(n)$, il existe des algorithmes en **temps exponentiel**.
— Pour $\gamma = 2^{\mathcal{O}(n)}$, l'algorithme **LLL** permet de le résoudre en **temps polynomial**.

Un autre problème important concerne la recherche de vecteurs proches d'une cible dans un réseau.

— **Closest Vector Problem (CVP)** : Étant donnés une cible $t \in \mathbb{R}^n$ et un réseau $\mathscr{L}(B)$, trouver un vecteur $v \in \mathscr{L}$ tel que

$$\|t - v\| = d(t, \mathscr{L}) := \min\{\|t - v\| \text{ tel que } v \in \mathscr{L}\}.$$

De même, on peut considérer une version approximative :

— **CVP**$_\gamma$, où $\gamma > 0$: Trouver un vecteur $v \in \mathscr{L}$ tel que

$$\|t - v\| \leq \gamma \cdot d(t, \mathscr{L}).$$

Le problème **CVP** est en général difficile pour un réseau arbitraire. Cependant, pour certaines familles spécifiques de réseaux, comme $\mathbb{Z}^n$, des algorithmes en temps polynomial sont connus. La qualité de la base choisie joue un rôle crucial dans la résolution du problème.

Théorème 1.4. Il existe un algorithme qui résout **CVP**$_{\exp(n)}$ en temps polynomial via l'algorithme **LLL**.

L'efficacité des algorithmes dépend grandement de la qualité de la base du réseau euclidien choisie. Le chapitre suivant abordera des techniques pour améliorer la base, via l'algorithme **LLL**.

1.2 Réseaux polynomiaux

Lorsque les coefficients des matrices appartiennent à un corps $\mathbb{K}$, les opérations classiques telles que la multiplication, l'inversion, le calcul du déterminant ou la résolution de systèmes linéaires possèdent des complexités relativement comparables. En revanche, lorsqu'on considère des matrices à coefficients polynomiaux (dans $\mathbb{K}[x]$), certaines différences notables apparaissent : si le calcul du déterminant conserve une complexité voisine de celle du produit matriciel, l'inversion de matrices polynomiales est sensiblement plus coûteuse, principalement en raison de la croissance significative des degrés intermédiaires des résultats. Cette complexité accrue découle de la structure algébrique particulière de l'anneau $\mathbb{K}[x]$: en effet, bien qu'il s'agisse d'un anneau principal (à la différence de $\mathbb{K}[x, y]$), il ne s'agit pas d'un corps. Par conséquent, certaines opérations familières dans un corps, comme l'inversion générale d'un élément non nul, ne sont plus systématiquement réalisables. Notamment, dans $\mathbb{K}[x]$, seuls les polynômes constants non nuls sont inversibles. Cette restriction impose de repenser ou de redéfinir rigoureusement plusieurs notions classiques de l'algèbre linéaire lorsqu'on manipule des matrices polynomiales. Malgré ces difficultés, les matrices à coefficients dans $\mathbb{K}[x]$ demeurent essentielles dans de nombreuses applications, en particulier pour l'interpolation bivariée, une étape centrale du décodage des codes de Reed-Solomon. Pour des rappels détaillés sur les anneaux, le lecteur est invité à consulter l'annexe correspondante.

1.2.1 Généralités

Définition 1.5. Un **réseau polynomial** est un $\mathbb{K}[x]$-module libre de type fini.

Remarque. Un réseau polynomial admet donc une base, un rang.

Notation. $\mathbb{K}[x]^{m \times n}$ est l'ensemble des matrices $m \times n$ à coefficients dans $\mathbb{K}[x]$, elles sont appelées **matrices polynomiales**.

Exemple.

$$\begin{pmatrix} 3x + 4 & 4x^2 + 3 \\ 5 & 3x^2 + 1 \end{pmatrix} \in \mathbb{K}[x]^{2 \times 2}$$

est une matrice polynomiale.

On observe une analogie structurelle entre les matrices et les modules : de même que les matrices à coefficients dans $\mathbb{K}$ sont naturellement liées aux $\mathbb{K}$-espaces vectoriels, les matrices à coefficients dans $\mathbb{K}[x]$ interviennent de manière équivalente dans l'étude des $\mathbb{K}[x]$-modules libres.

1.2.2 Complexité

Dans la suite, nous allons considérer les opérations usuelles sur les matrices à coefficients dans $\mathbb{K}[x]$. Lorsque ces opérations ne sont pas directement définies dans $\mathbb{K}[x]$, on les effectue dans son corps de fractions $\mathbb{K}(x)$, ce qui permet notamment de parler d'inversion ou de résolution de systèmes linéaires.

Proposition 1.4. On a une inclusion naturelle :

$$\mathbb{K}[x]^{m\times n} \subset \mathbb{K}(x)^{m\times n}$$

où $\mathbb{K}(x)^{m\times n}$ désigne l'ensemble des matrices à coefficients dans le corps des fractions $\mathbb{K}(x)$.

Proposition 1.5. L'addition dans $\mathbb{K}[x]^{m\times n}$ coûte mn additions dans $\mathbb{K}[x]$.

Question : Quelle est la complexité de l'addition naïve dans $\mathbb{K}[x]^{m\times m}$?
Question : Quelle est la complexité de la multiplication naïve dans $\mathbb{K}[x]^{m\times m}$?

Notation. Soit $2 < \omega < 3$ tel que l'on puisse multiplier deux matrices $m \times m$ sur un anneau commutatif en $\mathcal{O}(m^\omega)$ opérations dans l'anneau.

Que peut-on en déduire sur le coût de la multiplication de deux matrices dans $\mathbb{K}[x]^{m\times m}$?
Ce point de vue est difficilement utilisable, il conduit facilement à des bornes de coût non pertinentes, par exemple l'addition dans $\mathbb{K}[x]^{m\times n}$ coûte mn additions dans $\mathbb{K}(x)$.

1.3 Deux points de vue sur les matrices polynomiales

Théorème 1.5. On dispose d'un **isomorphisme structurel** au sens des modules :

$$\mathbb{K}[x]^{m\times n} \;\cong\; \mathbb{K}^{m\times n}\big[x\big]$$

Remarque. Une matrice polynomiale peut être interprétée soit comme un ensemble de polynômes dans $\mathbb{K}[x]$, soit comme un polynôme (en x) à coefficients dans l'anneau matriciel $\mathbb{K}^{m\times n}$. Le choix de l'approche dépend alors principalement du type de calculs et d'estimations de complexité qu'on souhaite mener.

Exemple.

$$\begin{pmatrix} x^3+4x+1 & 4x^2+3 \\ 5x^2+3x+1 & 5x+3 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 5 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} x + \begin{pmatrix} 0 & 0 \\ 0 & 5 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} x^3$$

Lorsque les matrices possèdent des coefficients dans $\mathbb{K}[x]$, deux approches principales sont envisageables pour effectuer des calculs algébriques (résolution de systèmes, inversion, déterminant, etc.) :

1. **Appliquer directement les algorithmes d'algèbre linéaire classique** $\mathbb{K}[x]$
   On traite la matrice comme un objet usuel, en considérant simplement que les coefficients se trouvent dans l'anneau principal $\mathbb{K}[x]$.

— *Avantage* : cette méthode tire parti de la robustesse théorique et de l'expérience accumulée avec les algorithmes classiques (résolution de systèmes linéaires, inversion, etc.).
— *Limite* : on peut rapidement générer des calculs complexes, par exemple des fractions polynomiales de grand degré, et obtenir des bornes de complexité peu réalistes si l'on n'exploite pas la structure polynomiale de manière fine.

2. **Voir la matrice comme un polynôme à coefficients matriciels**($(\mathbb{K}^{m\times n})[x]$) Cette optique mobilise des algorithmes d'arithmétique polynomiale, permettant un meilleur contrôle du degré lors des opérations.
— *Avantage* : on bénéficie de techniques optimisées pour les polynômes (évaluation-interpolation, accélération de la multiplication via FFT, etc.).
— *Limite* : le fait de tout considérer sous forme de polynôme à coefficients matriciels peut parfois s'avérer restrictif[4] ou inefficace[5] , en particulier si les degrés des entrées diffèrent sensiblement d'une ligne ou d'une colonne à l'autre.

1.3.1 Analyse fine de la complexité

La multiplication dans $\mathbb{K}[x]^{m\times m}$ avec un degré $\leq d$: $\mathcal{O}(d\log d)$ multiplications dans $\mathbb{K}^{m\times m}$ $\mathcal{O}(d\log d\log\log d)$ additions dans $\mathbb{K}^{m\times m}$
On en déduit que : $\mathrm{MM}(m,d)\in\mathcal{O}(m^\omega d\log d + m^2 d\log d\log\log d)$

Remarque. Une approche efficace pour inverser une matrice polynomiale sur $\mathbb{K}[x]$ repose sur la stratégie *évaluation-inversion-interpolation* (ou *eval-inv-éval*), utilisant la transformée de Fourier rapide (FFT) pour accélérer les calculs. Cette méthode, décrite par Bostan et Schost Bostan et Schost 2005, permet d'atteindre une complexité en :

$$\mathcal{O}(m^\omega d + m^2\log d),$$

où m est la taille de la matrice, d le degré des polynômes, et ω l'exposant de la multiplication matricielle.

Définition 1.6. Soit $A\in\mathbb{K}[x]^{m\times n}$, la **taille** de A, notée $\mathrm{size}(A)$, est le nombre de coefficients distincts de $\mathbb{K}$ nécessaires pour sa représentation dense.
Et on a la relation

$$\mathrm{size}(A)=\sum_{i,j}\mathrm{size}(a_{i,j})=\sum_{i,j}(1+\max(0,\deg(a_{i,j}))).$$

Exemple. Considérons les matrices de degrés :

$$\begin{pmatrix}[100] & [50] & [10]\\ [100] & [50] & [10]\\ [100] & [50] & [10]\end{pmatrix}\begin{pmatrix}[50] & [50] & [50]\\ [50] & [50] & [50]\\ [50] & [50] & [50]\end{pmatrix}=\begin{pmatrix}[150] & [150] & [150]\\ [150] & [150] & [150]\\ [150] & [150] & [150]\end{pmatrix}$$

Remarque. En général, la taille n'est pas compatible avec le produit matriciel, mais cela peut être le cas dans certains cas particuliers.

4. Dans la division avec reste, on suppose souvent que la matrice B possède un coefficient dominant inversible ($\mathrm{lc}(B)\neq 0$). On pourrait toutefois assouplir cette hypothèse en imposant plutôt que B soit «réduite» ou non singulière, mais cela sortirait du cadre habituel.

5. Si l'on travaille avec une matrice de degré d dont de nombreuses entrées ont un degré bien inférieur à d, les algorithmes basés uniquement sur le degré maximal risquent de fournir des performances dégradées. Une analyse plus précise devrait tenir compte des degrés individuels, ou plus globalement du degré de chaque ligne et colonne.

Rappelons que $\deg(AB) \leq \deg(A) + \deg(B)$.
Les mesures de degré introduites précédemment, ainsi que les techniques associées, permettent d'accélérer certains algorithmes dans des cas spécifiques. Toutefois, plusieurs limitations structurelles demeurent.

— Les degrés de lignes et de colonnes ne se comportent pas bien vis-à-vis de la multiplication matricielle.
— L'hypothèse restrictive selon laquelle le coefficient dominant $\mathrm{lc}(B)$ est inversible reste difficile à lever dans la division avec reste.
— Des questions ouvertes subsistent concernant la possibilité de concevoir des algorithmes plus rapides pour le calcul du déterminant ou de l'inverse d'une matrice polynomiale.

Ces difficultés soulignent l'intérêt de la réduction des matrices polynomiales, qui constitue un outil essentiel pour mieux contrôler la croissance des degrés et améliorer l'efficacité algorithmique.

CHAPITRE 2

Réduction de réseaux

La réduction de réseaux joue un rôle central en cryptographie, car la difficulté à trouver une « bonne base » d'un réseau est précisément ce qui assure la robustesse de nombreux systèmes cryptographiques actuels et post-quantiques. La réduction consiste à transformer une base arbitraire en une base mieux adaptée aux calculs, c'est-à-dire constituée de vecteurs courts et quasi orthogonaux dans le cas des réseaux euclidiens. Cependant, la complexité algorithmique de ce processus varie considérablement selon la nature du réseau étudié :

— La réduction exacte de réseaux définis sur $\mathbb{F}_p[x]$ peut être réalisée efficacement, en temps polynomial.

— En revanche, la réduction exacte des réseaux définis sur $\mathbb{Z}$ est un problème connu pour être NP-difficile.

Ce chapitre est dédié à l'étude approfondie de ces deux types de réduction. Nous commencerons par examiner en détail les méthodes de réduction pour les réseaux polynomiaux, ce qui nous permettra de mieux identifier les obstacles intrinsèques à la réduction efficace des réseaux euclidiens, et d'en comprendre les implications cryptographiques.

2.1 Réduction de réseaux polynomiaux

Autrement dit, deux bases d'un module sur $\mathbb{F}[x]$ ne diffèrent que par une multiplication à gauche par une matrice inversible (unimodulaire).

La réduction des réseaux polynomiaux est une étape essentielle dans plusieurs applications algorithmiques, en particulier dans le décodage efficace des codes de Reed-Solomon généralisés. Cette opération vise à transformer une base quelconque d'un réseau polynomial en une base simplifiée ou réduite, facilitant ainsi les calculs ultérieurs. Dans cette section, nous détaillerons les principaux concepts, outils et algorithmes permettant de réaliser cette réduction en temps polynomial, en mettant l'accent sur les approches les plus performantes actuellement connues. Nous ferons ainsi un état de l'art des avancées récentes en matière de complexité et d'efficacité algorithmique, tout en discutant des défis encore ouverts dans le domaine.

On notera $\mathbb{K}$ un corps quelconque.

2.1.1 Généralités

Soit $F \in \mathbb{F}[x]^{m\times n}$. On définit $(F,\sigma) := \{v \in \mathbb{F}[x]^{1\times m}$ tel que $vF = 0 \mod x^\sigma\}$. On appellera σ la **précision**.

Proposition 2.1. (F,σ) est un $\mathbb{F}[x]$-module de dimension m.

Définition 2.1. Une (F,σ)-**base d'ordre** est une base (au sens des $\mathbb{F}[x]$-modules) de (F,σ) de degré minimale.

Quelle est la définition du degré ? Que signifie "minimale" dans ce contexte ?

Définition 2.2. On a les définitions suivantes pour le degré en ligne :

— Pour un vecteur ligne $M \in \mathbb{K}[x]^{1\times n}$, on définit son **degré en ligne** par :

$$\mathrm{rdeg}(M) = \max_{1\le i\le n} \deg(m_i)$$

où m_i désigne les éléments de M.

— Pour une matrice $M \in \mathbb{K}[x]^{n\times n}$, on définit son **degré en ligne** comme le maximum des degrés de ligne de ses lignes :

$$\mathrm{rdeg}(M) = \max_{1\le i\le n} \mathrm{rdeg}(M_i)$$

où M_i désigne la i-ième ligne de M considérée comme un vecteur ligne.

Exemple. Soit $M = \begin{pmatrix} 1 & 0 & 1 \\ x & 1 & x+1 \\ 1 & x^3+x^2 & x \end{pmatrix} \in \mathbb{F}_2[x]$. Alors $\mathrm{rdeg}(M) = \begin{pmatrix} 0 & 1 & 3 \end{pmatrix}$.

Cette définition du degré de ligne présente une limite : si $c = bA$, on a bien en général $\mathrm{rdeg}(c) \le \mathrm{rdeg}(b) + \mathrm{rdeg}(A)$, mais cette majoration est souvent trop lâche pour nos besoins. Ce qui nous intéresse est de pouvoir caractériser plus finement le degré de c, voire d'obtenir une égalité. Cela motive l'introduction d'une nouvelle définition.

Définition 2.3. Soit $s \in \mathbb{Z}^n$.

— Pour un vecteur ligne $M \in \mathbb{K}[x]^{1\times n}$, on définit son **degré en ligne décalé** par :

$$\mathrm{rdeg}_s(M) = \max_{1\le i\le n} (\deg(m_i) + s_i)$$

où m_i désigne les éléments de M.

— Pour une matrice $M \in \mathbb{K}[x]^{m\times n}$, on définit son **degré en ligne décalé** comme le vecteur des degrés de ligne décalés de ses lignes :

$$\mathrm{rdeg}_s(M) = \big(\mathrm{rdeg}_s(M_i)\big)_{1\le i\le m} \in \mathbb{Z}^m$$

où M_i désigne la i-ième ligne de M considérée comme un vecteur ligne.

Notation. Soit $s \in \mathbb{Z}^n$. On note x^s par la matrice diagonale $\begin{pmatrix} x^{s_1} & & \\ & \ddots & \\ & & x^{s_n} \end{pmatrix}$

Proposition 2.2. Soit $A \in \mathbb{K}[x]^{m\times n}$, et $s \in \mathbb{Z}^n$ un vecteur de décalage. Le degré de ligne décalé de A satisfait la relation $\mathrm{rdeg}_s(A) = \mathrm{rdeg}(Ax^s)$.

Exemple. Soit

$$F = \begin{pmatrix} 1 & 0 & 1 \\ x & 1 & x+1 \\ 1 & x^3+x^2 & x \end{pmatrix} \in \mathbb{F}_2[x] \quad \text{et} \quad s = (1,0,0,1)$$

Alors

$$\mathrm{rdeg}_s(F) = \mathrm{rdeg}(F \cdot x^s) = \mathrm{rdeg} \begin{pmatrix} x & 0 & 1 \\ x^2 & 1 & x+1 \\ x & x^3+x^2 & x \end{pmatrix} \in \mathbb{F}_2[x] = (1,2,3,4)$$

Proposition 2.3. Soit $A \in \mathbb{K}[x]^{m\times n}$ et $s \in \mathbb{Z}^n$ un vecteur de décalage.
Alors, on a les propriétés suivantes :

— $\mathrm{rdeg}_s(A) = v$ si et seulement si $\mathrm{rdeg}(x^{-v}Ax^s) = 0$.
— $\mathrm{rdeg}_s(A) \leq v$ si et seulement si $\mathrm{rdeg}(x^{-v}Ax^s) \leq 0$.

Exemple. Soit

$$F = \begin{pmatrix} 1 & 0 & 1 \\ x & 1 & x+1 \\ 1 & x^3+x^2 & x \end{pmatrix}, \quad u = (1,0,0,1).$$

Alors

$$v = \mathrm{rdeg}_u(F) = (1,2,3,4) \quad \text{et} \quad x^{-v}Ax^u = \begin{pmatrix} 1 & 0 & x^{-1} \\ 1 & x^{-2} & x^{-2}+x^{-1} \\ x^{-2} & x^{-1}+1 & x^{-2} \end{pmatrix}.$$

Proposition 2.4. Soit $A \in \mathbb{K}[x]^{m\times n}$, $b \in \mathbb{K}[x]^{1\times m}$ et $c = bA$. Soit $v = \mathrm{rdeg}_u(A)$ et $w = \mathrm{rdeg}_v(b)$. Alors

$$\mathrm{rdeg}_u(c) \leq w.$$

On va définir un ordre sur les degrés de ligne, bien que non total.

Définition 2.4. Soit $m \in \mathbb{N}^*$ et soient $u = (u_1, \ldots, u_m)$, $v = (v_1, \ldots, v_m) \in \mathbb{Z}^m$ deux vecteurs de degrés de ligne, triés par valeur croissante. On définit une relation d'ordre partiel, notée $\leq_{ob}$ (ordre obtenu par composantes), par :

$$u \leq_{ob} v \quad \text{si et seulement si} \quad u_i \leq v_i \quad \text{pour tout } i \in \{1, \ldots, m\}.$$

Définition 2.5. Soit $F \in \mathbb{F}[x]^{m\times n}$. On dit que F est **réduite par ligne** si, pour tout $U \in \mathbb{F}[x]^{m\times m}$ unimodulaire, on a : $\mathrm{rdeg}(F) \leq_{ob} \mathrm{rdeg}(UF)$.

On remarque que pour parler d'un minimum, il faudrait un ordre total. On peut enfin voir la nouvelle définition.

Définition 2.6. Une base d'ordre est une base du $\mathbb{F}[x]$-module (F, σ) qui est réduite par ligne.

Proposition 2.5. Il existe une base réduite par ligne de (F, σ).

Exemple. $$\begin{pmatrix} 1 & 0 & 1 \\ x & 1+x & 0 \\ x^2+x^3 & x & 0 \end{pmatrix} \cdot \begin{pmatrix} x+x^2+x^3+x^4+x^5+x^6 \\ 1+x+x^5+x^6+x^7 \\ 1+x^2+x^4+x^5+x^6+x^7 \end{pmatrix} = 0^{4\times 1} \mod x^8$$

L'existence d'une base réduite est garantie, mais elle n'est pas nécessairement unique. Pour assurer l'unicité, une condition supplémentaire est requise : la forme de Popov.

Preuve naïve (incorrecte). Considérons le minimum de tous les $\mathrm{rdeg}(PU)$ triés, pour toutes les matrices unimodulaires $U \in \mathbb{F}[x]^{m\times m}$.
Toute base PU ayant un degré minimal est une base d'ordre. Attention : l'ordre $\leq_{ob}$ n'est pas un ordre total. En effet, il est possible d'avoir deux bases dont les degrés en ligne sont respectivement $(1,2,3)$ et $(1,1,4)$. On ne peut pas encore garantir l'existence d'un minimum ! ■

Définition 2.7. Soit $A \in \mathbb{F}[x]^{m\times n}$ et soit $v = \mathrm{rdeg}_u(A)$. On définit la **matrice des coefficients dominants** de A, notée $\mathrm{lcoeff}(A) \in \mathbb{F}^{m\times n}$, comme étant la matrice obtenue en extrayant la partie constante de $x^{-v}Ax^s$, c'est-à-dire :

$$\mathrm{lcoeff}(A) = \lim_{x\to\infty} x^{-v}Ax^s.$$

Exemple. Soit

$$F = \begin{pmatrix} 1 & 0 & 1 \\ x & 1 & 1+x \\ 1 & x^2+x^3 & x \end{pmatrix}.$$

Alors

$$\vec{v} := \mathrm{rdeg}(F) = (1,2,3) \quad \text{et} \quad x^{-\vec{v}} \cdot A \cdot x^{\vec{s}} = \begin{pmatrix} 1 & 0 & x^{-1} \\ 1 & x^{-2} & x^{-2}+x^{-1} \\ x^{-2} & x^{-1}+1 & x^{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \mathcal{O}_{x\to\infty}(x^{-1})$$

Proposition 2.6 (Transitivité, revisitée)**.** Soient $c := b \cdot A$, $v = \mathrm{rdeg}_u(A)$ et $w = \mathrm{rdeg}_v(b)$.
Si $\mathrm{lcoeff}(A)$ est **injective à gauche**, alors $\mathrm{rdeg}_u(c) = w$.

Proposition 2.7. Soit A une matrice. Si $\mathrm{lcoeff}(A)$ est injective à gauche, alors A est réduite par ligne.

Question : Comment réduire par ligne une matrice ?

Notation. On note $[d]$ un polynôme de degré d.

On définit le pivot d'une ligne comme l'élément non nul de degré maximal le plus à droite dans cette ligne.

Définition 2.8. Soit $W \in \mathbb{F}[x]^{m\times n}$. La matrice W est dite en **forme Popov faible** si chaque ligne de W possède un pivot, et si les indices de colonnes de ces pivots sont distincts deux à deux.

Exemple. La matrice

$$W = \begin{pmatrix} [1] & [1] & [1] \\ [2] & [1] & [1] \\ [1] & [2] & [2] \end{pmatrix}$$

est en forme Popov faible , car les pivots, en rouge, ont des indices distincts.

Pour transformer une matrice en forme Popov faible, on peut utiliser l'algorithme de Mulders et Storjohann 2003, qui fournit une méthode systématique pour y parvenir.

Proposition 2.8. Toute matrice en *forme Popov faible* est réduite par ligne.

Algorithme 1 : Weak-Popov

Entrée : $A \in \mathbb{F}[x]^{m\times n}$
Sortie : La forme de Popov faible de A
while *deux lignes ont le même indice de pivot* **do**
  Ajouter des multiples d'un monôme d'une ligne à une autre afin de :;
  - déplacer un pivot vers la gauche, ou;
  - diminuer le degré d'une ligne.;

Théorème 2.1. La complexité de l'algorithme *Weak-Popov* est $\mathcal{O}(m^3d^2)$.

Exemple.

$$\begin{pmatrix} [3] & [3] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} [3] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} [2] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{pmatrix}$$

1. Ajouter $*x^2$ fois la deuxième ligne à la première ligne (avec un $* \in \mathbb{F}$ approprié).

2. Ajouter $*$ fois la dernière ligne à la première ligne.

La matrice finale est en forme Popov faible, les pivots ont des indices distincts.

Proposition 2.9 (Changement de base)**.** Soient P et Q deux bases de lignes d'un même $\mathbb{F}[x]$-module libre (avec $\mathbb{F}$ un corps). Alors, il existe une matrice unimodulaire U telle que

$$P \;=\; U\,Q.$$

2.1.2 Algorithmes de réduction de réseaux polynomiaux

On s'intéresse maintenant à des algorithmes efficaces pour calculer des bases d'ordre.

Cas initial quand $\sigma = 1$ On peut d'abord étudier un algorithme pour calculer une base d'ordre dans le cas de base $\sigma = 1$, c'est-à-dire lorsque les polynômes sont constants. Nous nous plaçons dans l'hypothèse où $\sigma = 1$. Soit $F \in \mathbb{F}^{m\times n}$, nous cherchons une base du module (F, σ).

On remarque que si $\begin{pmatrix} S \\ K \end{pmatrix} F = \begin{pmatrix} R \\ 0 \end{pmatrix}$ avec R de rang maximal, alors $\begin{pmatrix} xS \\ K \end{pmatrix} F = \begin{pmatrix} xR \\ 0 \end{pmatrix} = 0 \mod x$ ce qui implique que $\begin{pmatrix} xS \\ K \end{pmatrix}$ est une base du module $(F, 1)$.

Les candidats naturels pour S et K sont les suivants : K est le noyau et S est le supplémentaire du noyau. On pourra choisir le noyau K utilisant les lignes de F de plus petit degré, une façon de les calculer consiste à obtenir la forme échelonnée par lignes de F. Cela nous donne l'algorithme suivant, qui sera utilisé lorsque $\sigma = 1$.

Algorithme 2 : Basis

Entrée : $F \in (\mathbb{F}[x]_{\leq 0})^{m\times n}$, et un vecteur de décalage s
Sortie : Une $(F, 1, s)$-base d'ordre et son degré de ligne s
On suppose que s est croissant.;
Calculer une forme ligne échelonnée $F = \tau \cdot L \cdot E$ avec :;
$r = \mathrm{rang}(E)$,
τ une permutation,
$L = \begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix}$ triangulaire inférieure,
$\begin{pmatrix} E' \\ 0 \end{pmatrix} E =$ ligne échelonnée.;
return $\begin{pmatrix} xL_r & 0 \\ G & I_{m-r} \end{pmatrix}$, $\tau^{-1}s + [1_r, 0_{n-r}]$

Cas général Maintenant, on va devoir découper le problème pour trouver une base d'ordre pour $\sigma > 1$.

On présente un algorithme quadratique qui fonctionne de façon itérative : $(F, 1) \to \cdots \to (F, \sigma)$

Algorithme 3 : M-Basis

$P_0 \leftarrow$ ***Basis***$(F \bmod x)$;
for k *de* 1 *à* $\sigma - 1$ **do**
  $F' \leftarrow x^{-k} P_{k-1} F$;
  $M_k \leftarrow$ ***Basis***$(F' \bmod x)$;
  $P_k \leftarrow M_k P_{k-1}$;
return $P_{\sigma-1}$

On présente maintenant un algorithme quasi-linéaire qui fonctionne sur le principe diviser-pour-régner.

Algorithme 4 : PM-Basis

if $\sigma = 1$ **then**
  return Basis$(F \bmod x)$
else
  $P_{\text{low}} \leftarrow$ PM-Basis$(F, \lfloor \sigma/2 \rfloor)$;
  Soit F' tel que $P_{\text{low}} F = xF'$;
  $P_{\text{high}} \leftarrow$ PM-Basis$(F', \lfloor \sigma/2 \rfloor)$;
  return $P_{high} \cdot P_{low}$

Théorème 2.2. La complexité de l'algorithme *PM-Basis* est $\mathcal{O}(\mathrm{MM}(m, \sigma) \log(\sigma))$.

2.2 Réduction de réseaux euclidiens

Dans cette section, nous nous concentrerons sur un algorithme de réduction de réseau s'exécutant en temps polynomial : l'algorithme LLL, du nom de ses auteurs A. Lenstra, H. Lenstra et L. Lovász. Nous ne traiterons pas d'autres algorithmes plus avancés comme BKZ, afin de rester dans un cadre plus élémentaire. L'algorithme LLL repose sur une idée simple mais puissante : il produit une approximation entière de la décomposition de Gram-Schmidt et réorganise les vecteurs de la base pour en améliorer la structure. Le lecteur souhaitant se rafraîchir la mémoire sur le procédé d'orthogonalisation de Gram-Schmidt est invité à consulter l'annexe dédiée. Celui-ci ne sera pas rappelé ici afin de préserver la concision du texte.

2.2.1 Notion fondamentale de LLL : base réduite

Définition 2.9. Soit $b_1, \dots, b_n$ une base d'un réseau et U la matrice triangulaire supérieure telle que $B = B^*U$ est dite **propre**[1] si

$$\max_{1 \leq i < j \leq n} |\mu_{ij}| \leq \frac{1}{2}. \tag{2.1}$$

Cette condition garantit une forme de quasi-orthogonalité entre les vecteurs de la base B^*. En effet, l'inégalité (2.1) implique que l'angle entre deux vecteurs consécutifs est compris entre $60°$ et $120°$, ce qui signifie qu'ils sont presque orthogonaux deux à deux. Pour une justification plus détaillée, notamment à travers l'étude de la matrice de Gram, le lecteur est invité à consulter l'annexe correspondante.

Définition 2.10. Soit $\mathcal{B}$ une base de $\mathbb{R}^n$ et $\mathcal{B}^*$ sa base de Gram-Schmidt associée.
On dit que la famille $(b_1, \dots, b_n)$ est **réduite**[2] si

$$\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2 \text{ pour } 1 \leq i \leq n$$

On dit que la famille $(b_1, \dots, b_n)$ satisfait la **condition de Lovász** si

$$(\delta - \mu_{i+1,i}^2)\,\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2 \text{ pour } 1 \leq i \leq n, \text{ où } \delta \in \left]\frac{1}{4}, 1\right]$$

Définition 2.11. Une base $b_1, \dots, b_n$ d'un réseau est dite **réduite** (resp. **LLL-réduite**) si

— elle est propre.
— elle est réduite (resp. satisfait la condition de Lovàsz).

Remarque. Chaque vecteur de la base réduite a une norme au moins égale à la moitié de celle du précédent, garantissant ainsi une décroissance modérée.

Théorème 2.3. Soit $\mathcal{B}$ une base réduite du réseau $\mathscr{L} \subseteq \mathbb{R}^n$ et soit $v \in \mathscr{L} \setminus \{0\}$. Alors $\|b_1\| \leq 2^{(n-1)/2} \cdot \|v\|$.

Théorème 2.4. Soit $\mathcal{B}$ une base du réseau $\mathscr{L} \subseteq \mathbb{R}^n$ qui satisfait la condition de Lovász et soit $v \in \mathscr{L} \setminus \{0\}$. Alors $\|b_1\| \leq \frac{1}{(\delta - \mu_{i+1,i}^2)^{\frac{n-1}{2}}}\|v\|$, si le dénominateur ne s'annule pas.

1. Une base propre est aussi connue sous le nom de base size-réduite dans la littérature.
2. Aussi connu sous le nom de base **SIEGEL-réduite** dans la littérature

2.2.2 LLL : fonctionnement

Algorithme 5 : *BasisReduction*

Entrée : Une base $B = (f_1, \dots, f_n)$
Sortie : Une base réduite $G = (g_1, \dots, g_n)$ de B
for $i = 1$ **to** n **do**
  $g_i \coloneqq f_i$;
$(B^*, U) \coloneqq \text{GSO}\ (B)$;
while $i \leq n$ **do**
  for $j = i-1, i-2, \dots, 1$ **do**
    $g_i \coloneqq g_i - \lceil \mu_{ij} \rfloor\ g_j$;
    Mettre à jour $(B^*, U) \coloneqq \text{GSO}\ (B)$;
  if $i > 1$ ***et*** $\|f_i^*\|^2 > 2\|f_{i+1}^*\|^2$ **then**
    Échanger g_{i-1} et g_i;
    Mettre à jour $(B^*, U) \coloneqq \text{GSO}\ (B)$;
    $i \coloneqq i - 1$;
  else
    $i \coloneqq i + 1$;
return $G = (g_1, \dots, g_n)$

L'algorithme débute par le calcul de la base orthogonalisée de Gram-Schmidt, qui servira de support pour les opérations de réduction. Le principe consiste à appliquer successivement des étapes de réduction, en réorganisant les vecteurs de la base lorsqu'une certaine condition n'est pas respectée. Cependant, une application naïve de ces réductions ne garantit pas la terminaison de l'algorithme : il est nécessaire d'introduire un mécanisme de contrôle, comme la condition de Lovász, afin de déterminer quand effectuer un échange entre deux vecteurs. Cette condition assure la progression de l'algorithme et, in fine, sa terminaison.

Exemple. donner exemple

2.2.3 Correction, terminaison et de la complexité de LLL

Théorème 2.5 (Correction)**.** L'algorithme *BasisReduction (LLL)* calcule une base réduite de $\mathscr{L}$.

Nous aurons besoin de lemmes intermédiaires afin de prouver la correction. On commence par **étudier la proprification**. L'idée consiste à approcher au mieux, à l'aide d'entiers, les coefficients de la décomposition de Gram-Schmidt, de manière à construire une base réduite.

Notation. On définit l'entier le plus proche de $x \in \mathbb{R}$ par $\lceil x \rfloor = \lceil x + 1/2 \rfloor$.

Proposition 2.10. On a $|x - \lceil x \rfloor| \leq 1/2$ pour tout $x \in \mathbb{R}$.

On va maintenant regarder des étapes de *BasisReduction (LLL)*.

Algorithme 6 : *Proprification de* g_i

$g_i \coloneqq g_i - \lceil \mu_{ij} \rfloor \cdot g_j$;
Mettre à jour $(B^*, U) \coloneqq \text{GSO}(B)$;

Lemme 2.1.

1. Soit $G, G^*, M \in \mathbb{Q}^{n\times n}$ et $H, H^*, N \in \mathbb{Q}^{n\times n}$ les matrices des g_k, g_k^*, μ_{kl} avant et après *Proprification de* g_i. Soit $E = I_n - \lceil \mu_{ij} \rfloor E_{ij} \in \mathbb{Z}^{n\times n}$, où E_{ij} désigne la matrice élémentaire.
   Alors
   $$H = EG, \quad N = EM, \quad H^* = G^*.$$
2. Avant *Proprification de* g_i, on a :
   $$|\mu_{il}| \leq \frac{1}{2} \quad \text{pour} \quad j < l < i.$$

Preuve.

1. • *Proprification de* g_i se traduit matriciellement par $H = EG$.
   • La nouvelle famille est
   $$g_1, \ldots, g_{i-1}, g_i - \lceil \mu_{ij} \rfloor g_j, g_{i+1}, \ldots, g_n.$$
   On rappelle que i et j sont fixés et que $1 \leq j \leq i-1$. On a par définition du procédé de Gram-Schmidt $h_k^* = g_k^*$ pour $1 \leq k \leq i-1$.
   Pour $k = i$, on a
   $$h_i^* = h_i - \sum_{k=1}^{i-1} \frac{\langle h_i, h_k^* \rangle}{\|h_k^*\|^2} h_k^*$$
   $$= g_j - \lceil \mu_{ij} \rfloor g_j - \sum_{k=1}^{i-1} \frac{\langle g_i - \lceil \mu_{ij} \rfloor g_j, g_k^* \rangle}{\|g_k^*\|^2} g_k^*$$
   $$= g_i^* + \lceil \mu_{ij} \rfloor \sum_{k=1}^{i-1} \frac{\langle g_j, g_k^* \rangle}{\|g_k^*\|^2} g_k^* - \lceil \mu_{ij} \rfloor g_j$$
   $$= g_i^* + \lceil \mu_{ij} \rfloor \sum_{k=1}^{j} \frac{\langle g_j, g_k^* \rangle}{\|g_k^*\|^2} g_k^* - \lceil \mu_{ij} \rfloor g_j$$
   $$= g_i^* + \lceil \mu_{ij} \rfloor \sum_{k=1}^{j-1} \frac{\langle g_j, g_k^* \rangle}{\|g_k^*\|^2} g_k^* + g_j^* - \lceil \mu_{ij} \rfloor g_j = g_i^*$$
   Ainsi $h_i^* = g_i^*$. En poursuivant le procédé de Gram-Schmidt on en conclut $H^* = G^*$.
   • On a $NG^* \overset{(1)}{=} NH^* \overset{(D,1)}{=} H \overset{(1)}{=} EG \overset{(D,1)}{=} EMG^*$. En identifiant on a $N = EM$.
2. Au début de la boucle lorsque $j = i-1$ on a trivialement l'inégalité.
   La i-ème ligne de M
   $$(\mu_{i,1}, \cdots, \mu_{i,j}, \cdots, \mu_{i,i-1})$$
   Devient
   $$(\mu_{i,1} - \lceil \mu_{ij} \rfloor \mu_{j,1}, \cdots, \mu_{i,j} - \lceil \mu_{ij} \rfloor \mu_{j,j}, \cdots, \mu_{i,i-1} - \lceil \mu_{ij} \rfloor \mu_{j,i-1})$$
   $$(\mu_{i,1} - \lceil \mu_{ij} \rfloor \mu_{j,1}, \cdots, \mu_{i,j} - \lceil \mu_{ij} \rfloor, \cdots, \mu_{i,i-1})$$

■

Algorithme 7 : *Proprification de* $g_1, \ldots, g_{i-1}$

for $j = i-1, i-2, \ldots, 1$ **do**
  Proprification de g_i;

Lemme 2.2. *Proprification de* $g_1, \ldots, g_{i-1}$ ne change pas G^* et à la fin on a

$$|\mu_{il}| \leq \frac{1}{2} \text{ pour } 1 \leq l < i.$$

Preuve. D'après le lemme 2.1, après l'exécution de *Proprification de* $g_1, \ldots, g_{i-1}$, G^* n'a pas été modifié et en appliquant le lemme 2.1 pour $j = 1$ on a

$$|\mu_{il}| \leq \frac{1}{2} \text{ pour } 1 \leq l < i.$$

■

On étudie maintenant l'étape de réduction, l'idée consiste à réorganiser les vecteurs afin de garantir une progression quantifiable, qui assurera la terminaison de LLL.

Algorithme 8 : *Réduction de* g_{i-1}, g_i

if $i > 1$ ***et*** $\|f_i^*\|^2 > 2\left\|f_{i+1}^*\right\|^2$ **then**
  Échanger g_{i-1} et g_i;
  Mettre à jour $(B^*, U) \coloneqq \text{GSO}\ (B)$;
  $i \coloneqq i - 1$;
else
  $i \coloneqq i + 1$;

Lemme 2.3. Supposons que g_{i-1} et g_i sont échangés à l'étape *Réduction de* g_{i-1}, g_i.
On note h_k les vecteurs après échange et h_k^* leur base orthogonale de Gram-Schmidt.
Alors

1. $h_k^* = g_k^* \quad$ pour tout $k \in \{1, \ldots, n\} \setminus \{i-1, i\}$,
2. $\|h_{i-1}^*\|^2 < \frac{3}{4}\|g_{i-1}^*\|^2$,
3. $\|h_i^*\| \leq \|g_{i-1}^*\|$.

Preuve.

1. La famille

   $$g_1,\ \ldots,\ g_{i-2},\ g_{i-1},\ g_i,\ g_{i+1},\ \ldots,\ g_n$$

   devient

   $$h_1 \coloneqq g_1,\ \ldots,\ h_{i-2} \coloneqq g_{i-2},\ h_i \coloneqq g_i,\ h_{i-1} \coloneqq g_{i-1},\ h_{i+1} \coloneqq g_{i+1},\ \ldots,\ h_n \coloneqq g_n$$

   Par construction de Gram-Schmidt on a $h_k^* = g_k^*$ pour $1 \leq k \leq i-2$.
   On a

   $$h_{i+1}^* = h_{i+1} - \sum_{j=1}^{i} \frac{\langle h_{i+1}, h_j^* \rangle}{\left\|h_j^*\right\|^2} h_j^*$$

   $$= g_{i+1} - \sum_{j=1}^{i-2} \frac{\langle g_{i+1}, g_j^* \rangle}{\left\|g_j^*\right\|^2} g_j^* + \frac{\langle g_{i+1}, g_i^* \rangle}{\|g_i^*\|^2} g_i^* + \frac{\langle g_{i+1}, g_{i-1}^* \rangle}{\left\|g_{i-1}^*\right\|^2} g_{i-1}^* = g_{i+1}^*$$

   On en déduit donc que $h_k^* = g_k^*$ pour $i+1 \leq k \leq n$.
2. Le vecteur h_{i-1}^* est la composante de g_i orthogonale à $\sum_{1 \leq l < i-1} \mathbb{R} g_l$, or $g_i = g_i^* + \sum_{1 \leq l < i-1} \mu_{il} g_l^*$. Alors $h_{i-1}^* = g_i^* + \mu_{i,i-1} g_{i-1}^*$ et donc $\left\|h_{i-1}^*\right\|^2 = \|g_i^*\|^2 + \mu_{i,i-1}^2 \left\|g_{i-1}^*\right\|^2 \leq 1/2 \left\|g_{i-1}^*\right\|^2 + 1/4 \left\|g_{i-1}^*\right\|^2 = 3/4 \left\|g_{i-1}^*\right\|^2$.

3. Soit $u = \sum_{1 \leq \ell < i-1} \mu_{i-1,\ell} g_\ell^*$ et posons $U = \sum_{1 \leq \ell < i-1} \mathbb{R} g_\ell$ pour simplifier l'écriture.
   Alors, le vecteur h_i^* est la composante de $g_{i-1} = g_{i-1}^* + u$ orthogonale à $U + \mathbb{R} g_i$.
   Or $u \in U \subseteq U + \mathbb{R} g_i$.
   Alors, le vecteur h_i^* est la composante de g_{i-1}^* orthogonale à $U + \mathbb{R} g_i$.
   Par conséquent,
   $$\|h_i^*\| \leq \|g_{i-1}^*\|. \qquad \blacksquare$$

$\blacksquare$

Algorithme 9 : *LLL*

while $i \leq n$ **do**
  Proprification de $g_1, \ldots, g_{i-1}$;
  Réduction de g_{i-1}, g_i;

Lemme 2.4. Au début de chaque itération de la boucle à l'étape *LLL*, les invariants suivants sont vérifiés :

$$|\mu_{kl}| \leq \frac{1}{2} \quad \text{pour } 1 \leq l < k < i, \qquad \|g_{k-1}^*\|^2 \leq 2\|g_k^*\|^2 \quad \text{pour } 1 < k < i.$$

Preuve. Au début de l'étape *LLL*, les deux inégalités considérées sont satisfaites.

Supposons qu'elles restent vraies juste avant l'étape de *Proprification de* $g_1, \ldots, g_{i-1}$.

Le lemme 2.1 garantit que cette phase ne les altère pas : les inégalités demeurent donc valides après *Proprification de* $g_1, \ldots, g_{i-1}$.

Passons à l'étape *Réduction de* g_{i-1}, g_i. Un échange effectué durant cette réduction ne modifie aucun coefficient $\mu_{k\ell}$ avec $k < i - 1$; par conséquent, la première inégalité reste satisfaite. Par ailleurs, d'après le lemme 2.3, un échange ne modifie pas g_k^* pour $k \notin \{i - 1, i\}$, ce qui préserve la seconde inégalité.

Ainsi, à la fin de l'étape *Réduction de* g_{i-1}, g_i et donc au début de l'itération de *LLL* suivante les deux inégalités sont toujours vérifiées. Par récurrence sur les itérations, elles le sont à chaque instant de l'algorithme, ce qui conclut la démonstration. $\blacksquare$

Preuve de la correction. Le lemme 2.4 implique qu'à la fin de *LLL*, comme $i = n$, on a

$$|\mu_{kl}| \leq \frac{1}{2} \quad \text{pour } 1 \leq l < k < n, \qquad \|g_{k-1}^*\|^2 \leq 2\|g_k^*\|^2 \quad \text{pour } 1 < k < n.$$

ce qui prouve que la base est réduite. $\blacksquare$

Théorème 2.6 (Terminaison et complexité)**.** On pose $A = \max_{1 \leq i \leq n} \|f_i\|$. L'algorithme *BasisReduction (LLL)* termine et utilise $\mathcal{O}(n^4 \log A)$ opérations arithmétiques sur des entiers.

La difficulté est de montrer que la boucle Tant que ne va pas s'exécuter indéfiniment.

Lemme 2.5.

1. Orthogonalisation de Gram-Schmidt nécessite $\mathcal{O}(n^3)$ opérations dans $\mathbb{Z}$.
2. *Proprification de* $g_1, \ldots, g_{i-1}$ nécessite $\mathcal{O}(n^2)$ opérations dans $\mathbb{Z}$
3. *Réduction de* g_{i-1}, g_i nécessite $\mathcal{O}(n)$ opérations dans $\mathbb{Z}$

Preuve.

1. Il faut utiliser le théorème D.1
2. Une exécution de *Proprification de* g_i revient à faire les multiplications $H = EG$ et $N = EM$ se font en $\mathcal{O}(n)$ étapes, ainsi une exécution de *Proprification de* $g_1, \ldots, g_{i-1}$ nécessite $\mathcal{O}(n^2)$ opérations dans $\mathbb{Z}$.
3. Si un échange a lieu à *Réduction de* g_{i-1}, g_i, alors seuls g_{i-1}^*, g_i^*, ainsi que les lignes et colonnes $i-1$ et i de la matrice de transition M sont modifiés, et ces éléments peuvent être mis à jour en $O(n)$ opérations.

■

Il reste à borner le nombre d'itérations de la boucle Tant que à l'étape *LLL*.
Pour tout $1 \leq k \leq n$, on pose

$$G_k = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in \mathbb{Z}^{k \times n}, \quad d_0 = 1, \quad d_k = \det(G_k \cdot G_k^T) \in \mathbb{Z}.$$

Lemme 2.6. Pour tout $1 \leq k \leq n$, on a :

$$d_k = \prod_{1 \leq l \leq k} \|g_l^*\|^2 > 0.$$

Preuve. Soit $1 \leq k \leq n$, on définit G_k, U_k et G_k^* la décomposition de Gram-Schmidt de la famille $(g_i)_{1 \leq i \leq k}$
Alors

$$d_k = \det(G_k G_k^t) = \det(U_k G_k^*(G_k^*) t U_k^t) = \det(G_k^*(G_k^*)^t) = \prod_{1 \leq l \leq k} \|g_l^*\|^2 > 0$$

■

Lemme 2.7.

1. *Proprification de* $g_1, \ldots, g_{i-1}$ ne change pas d_k pour tout $1 \leq k \leq n$.
2. Si g_{i-1} et g_i sont échangés à l'étape *Réduction de* g_{i-1}, g_i, et si d_k^* désigne la nouvelle valeur de d_k, alors :

$$d_k^* = d_k \quad \text{pour tout } k \neq i-1, \quad \text{et} \quad d_{i-1}^* \leq \frac{3}{4} d_{i-1}.$$

Preuve.

1. D'après le lemme 2.2 *Proprification de* $g_1, \ldots, g_{i-1}$ ne modifie pas G_k^* et donc ne modifie pas d_k.
2. Pour $k \neq i-1$, une exécution de *Réduction de* g_{i-1}, g_i multiplie G_k par une matrice de permutation, donc $d_k^* = d_k$
   De plus, on a

$$d_{i-1} \overset{(2.6)}{=} \prod_{1 \leq l \leq i-1} \|g_l^*\|^2 \overset{(2.3)}{\leq} \frac{3}{4} \prod_{1 \leq l \leq i-1} \|h_l^*\|^2 \overset{(2.6)}{=} \frac{3}{4} d_{i-1}^*$$

■

On pose

$$D = \prod_{1 \leq k < n} d_k, \quad A = \max_{1 \leq i \leq n} \|f_i\|$$

On désigne D_0 désigne la valeur de D au début de l'algorithme, on a $1 \leq D \in \mathbb{Z}$ et

$$D_0 = \|f_1^*\|^{2(n-1)} \|f_2^*\|^{2(n-2)} \dots \|f_{n-1}^*\|^2$$

$$\leq \|f_1\|^{2(n-1)} \|f_2\|^{2(n-2)} \dots \|f_{n-1}\|^2 \leq A^{n(n-1)}$$

Puisque f_i^* est une projection de f_i pour tout i.

Lemme 2.8.

1. *Proprification de* $g_1, \dots, g_{i-1}$ ne modifie pas D.
2. D diminue d'au moins un facteur $3/4$ si un échange a lieu dans *Réduction de* g_{i-1}, g_i

Preuve.

1. D'après le lemme 2.7 *Proprification de* $g_1, \dots, g_{i-1}$ ne modifie pas d_k et donc ne modifie pas D.
2. Si g_{i-1} et g_i sont échangés lors de l'exécution de *Réduction de* g_{i-1}, g_i, en notant D^* la nouvelle valeur de D, alors d'après le lemme 2.7

$$d_k^* = d_k, \quad d_{i-1}^* \leq \frac{3}{4} d_{i-1} \text{ donc } D^* \leq \frac{3}{4} D.$$

■

À tout moment de l'algorithme, soit $e \in \mathbb{N}$ le nombre d'échanges effectués jusqu'à présent, et e^* le nombre de fois où la branche alternative (le *else*) dans *Réduction de* g_{i-1}, g_i a été prise.

Lemme 2.9. On a

$$e \leq \log_{4/3} D_0 \in \mathcal{O}(n^2 \log A)$$

Preuve. Soit D_e la valeur de D après e échanges.
On doit avoir

$$1 \ \leq \ D_e \ \leq \ \left(\frac{3}{4}\right)^e D_0 \leq \ \left(\frac{3}{4}\right)^e A^{n(n-1)}.$$

En appliquant $log_{3/4}$, aux extrémités de l'inégalité.

$$0 = \log_{3/4}(1) \ \geq \ e + \log_{3/4}(A^{n(n-1)}) = e + n(n-1)\frac{\log A}{\log(3/4)}.$$

On en déduit que $e \ \leq n(n-1)\frac{\log A}{-\log(3/4)}$ et donc $e \in \mathcal{O}(n^2 \log A)$

■

Preuve de la terminaison et la complexité.
Comme i est décrémenté de 1 lors d'un échange et incrémenté de 1 sinon l'entier $i+e-e^*$ est constant tout au long de *LLL*.
Initialement $i + e - e^* = 2$ et à la fin de *LLL* on a $n + 1 + e - e^* = 2$.
On en déduit donc que $e + e^* = 2e + n - 1 \in \mathcal{O}(n^2 \log A)$.
et donc d'après le lemme 2.5 le coût total de *LLL* est $\mathcal{O}(n^2 \times n^2 \log A)$ opérations dans $\mathbb{Z}$. Ce qui acheve la preuve. ■

Théorème 2.7. L'algorithme *BasisReduction (LLL)* opère sur des entiers dont la longueur est $\mathcal{O}(n \log A)$.

Il reste à montrer la dernière partie du théorème.

Lemme 2.10. Soit $g_1, \dots, g_n \in \mathbb{Z}^n$, et soit G^* et M respectivement la base de Gram-Schmidt et la matrice des coefficients associés. Pour tout $1 \leq l < k \leq n$, on a :

(i) $d_{k-1} g_k^* \in \mathbb{Z}^n$
(ii) $d_l \mu_{kl} \in \mathbb{Z}$
(iii) $|\mu_{kl}| \leq \sqrt{d_{l-1}} \|g_k\|$

Preuve.

1. On écrit
$$g_k^* = g_k - \sum_{1 \leq l < k} \lambda_{kl} g_l, \quad \lambda \in \mathbb{R}.$$
Soit $j < k$. On a
$$0 = \langle g_k^*, g_j \rangle = \left\langle g_k - \sum_{1 \leq l < k} \lambda_{kl} g_l, g_j \right\rangle.$$
Ce qui implique
$$\langle g_k, g_j \rangle = \sum_{1 \leq l < k} \lambda_{kl} \langle g_l, g_j \rangle$$
On a donc
$$\begin{pmatrix} \langle g_1, g_1 \rangle & \cdots & \langle g_{k-1}, g_1 \rangle \\ \vdots & & \vdots \\ \langle g_1, g_{k-1} \rangle & \cdots & \langle g_{k-1}, g_{k-1} \rangle \end{pmatrix} \begin{pmatrix} \lambda_{k1} \\ \vdots \\ \lambda_{kk-1} \end{pmatrix} = \begin{pmatrix} \langle g_k, g_1 \rangle \\ \vdots \\ \langle g_k, g_{k-1} \rangle \end{pmatrix}$$
D'après la règle de Cramer (à citer) on a
$$d_{k-1}\lambda_{k1} = \frac{\begin{vmatrix} \langle g_1, g_1 \rangle & \cdots & \langle g_{k-1}, g_1 \rangle \\ \vdots & & \vdots \\ \langle g_1, g_{k-1} \rangle & \cdots & \langle g_{k-1}, g_{k-1} \rangle \end{vmatrix}}{\begin{vmatrix} \langle g_1, g_1 \rangle & \cdots & \langle g_{k-1}, g_1 \rangle \\ \vdots & & \vdots \\ \langle g_1, g_{k-1} \rangle & \cdots & \langle g_{k-1}, g_{k-1} \rangle \end{vmatrix}} det(G_k G_k^t) = \begin{vmatrix} \langle g_1, g_1 \rangle & \cdots & \langle g_{k-1}, g_1 \rangle \\ \vdots & & \vdots \\ \langle g_1, g_{k-1} \rangle & \cdots & \langle g_{k-1}, g_{k-1} \rangle \end{vmatrix} \in \mathbb{Z}$$

2.
$$d_l \mu_{kl} = d_l \frac{\langle g_k, g_l^* \rangle}{\|g_l^*\|^2} = d_l \frac{\langle g_k, g_l^* \rangle}{d_l / d_{l-1}} = d_{l-1} \langle g_k, g_l^* \rangle = \langle g_k, g_l^* d_{l-1} \rangle \in \mathbb{Z}$$

3.
$$|\mu_{kl}| = \frac{\langle g_k, g_l^* \rangle^2}{\|g_l^*\|} \leq \frac{\|g_k\|}{\|g_l^*\|} \leq \sqrt{d_{l-1}/d_l} \|g_k\| \leq \sqrt{d_{l-1}} \|g_k\|$$

■

Nous avons supposé que $\|f_k\| \leq A$ pour tout k. Alors A est également une borne supérieure pour la base orthogonale de Gram-Schmidt initiale : $\|f_k^*\| \leq A$ pour tout k.
On a d'après les lemmes $\max \{\|g_k^*\| : 1 \leq k \leq n\}$ ne croît jamais au cours de l'algorithme. Ainsi, à tout instant et pour tout k, on a :

$$\|g_k^*\| \leq A \quad \text{et} \quad d_k = \prod_{1 \leq l \leq k} \|g_l^*\|^2 \leq A^{2k}.$$

Lemme 2.11. Soit $1 \leq k \leq n$.

1. À tout moment de l'algorithme, sauf éventuellement à l'étape *Proprification de* $g_1, \ldots, g_{i-1}$ lorsque $k = i$, on a :
$$\|g_k\| \leq \sqrt{n}A.$$
2. À chaque exécution de l'étape *Proprification de* g_i, on a :
$$\|g_i\| \leq n(2A)^n.$$

Preuve.

1. Initialement $\|g_k\| \leq A$ pour tout k. L'étape *Réduction de* g_{i-1}, g_i ne modifie pas $\|g_k\|$, il suffit donc d'examiner l'étape *Proprification de* $g_1, \ldots, g_{i-1}$. On a que g_k, pour $k \neq i$, n'est pas affecté par l'étape *Proprification de* g_i.
Soit $m_i = \max\{|\mu_{i\ell}| : 1 \leq \ell \leq i\}$. À partir de
$$g_i = \sum_{1 \leq \ell \leq i} \mu_{i\ell} g_\ell^*$$
et de l'orthogonalité des vecteurs g_ℓ^*, on obtient :
$$\|g_i\|^2 = \sum_{1 \leq \ell \leq i} \mu_{i\ell}^2 \|g_\ell^*\|^2 \leq n m_i^2 A^2, \quad \text{donc} \quad \|g_i\| \leq \sqrt{n}\, m_i A. \tag{4}$$
À la fin de *Proprification de* $g_1, \ldots, g_{i-1}$, on a $m_i = 1$ par le lemme 2.1.
2. Le lemme 2.10 et le point 1 impliquent qu'au début de *Proprification de* $g_1, \ldots, g_{i-1}$, on a
$$m_i \leq \max\left\{d_\ell^{1/2} : 1 \leq \ell \leq i\right\} \cdot \|g_i\| \leq A^{n-2} \cdot n^{1/2} A = n^{1/2} A^{n-1}. \tag{5}$$
Considérons maintenant le remplacement effectué à l'étape *Proprification de* g_i. Comme $m_i \geq 1$ et que $|\mu_{jl}| \leq \frac{1}{2}$ pour $1 \leq \ell < j$, le lemme 2.8 donne :
$$|\mu_{il} - \lfloor \mu_{ij} \rceil \mu_{jl}| \leq |\mu_{il}| + |\lfloor \mu_{ij} \rceil| \cdot |\mu_{jl}| \leq m_i + \left(m_i + \tfrac{1}{2}\right) \cdot \tfrac{1}{2} = \tfrac{3}{2} m_i + \tfrac{1}{4} \leq 2m_i$$
pour $1 \leq \ell < j$.
Pour $l = j$, la nouvelle valeur de μ_{ij} est par construction au plus $\frac{1}{2}$ en valeur absolue, tout comme les valeurs de μ_{il} pour $l > j$, d'après le lemme 2.1.
On en déduit que pour chaque valeur de j, la valeur de m_i est au plus doublée. Ainsi, pendant *Proprification de* $g_1, \ldots, g_{i-1}$, la valeur de m_i est multipliée au plus par un facteur $2^{i-1} \leq 2^{n-1}$. On a donc
$$m_i \leq n^{1/2}(2A)^{n-1}$$
Puis
$$\|g_i\| \leq n^{1/2} m_i A \leq n(2A)^n.$$

■

Preuve du theoreme.

— Les dénominateurs d_l des nombres rationnels calculés pendant l'algorithme sont au plus A^{2n}, et leur taille est en $\mathcal{O}(n \log A)$.
— Les numérateurs sont majorés en valeur absolue par :
  — $\|g_k\|_\infty \leq \|g_k\| \leq n(2A)^n$ d'après le lemme 2.11
  — $\|d_{k-1} g_k^*\|_\infty \leq \|d_{k-1} g_k^*\| \leq A^{2k-2} A \leq A^{2n}$ d'après le lemme 2.10
  — $|d_l \mu_{kl}| \leq d_l d_{l-1}^{1/2} \|g_l\| \leq A^{2l} A^{l-1} n(2A)^n \leq n(2A^4)^n$ d'après les lemmes 2.10 et 2.11

  et par conséquent, leur taille est aussi en $\mathcal{O}(n \log A)$.

■

CHAPITRE 3

Adaptation de la réduction de réseaux polynomiaux au cas entier

Dans ce chapitre, nous allons essayer d'adapter l'algorithme PM-Basis, pour les réseaux euclidiens.

CHAPITRE 4

Réseaux définis par relations plutôt que par générateurs

On considère ici les réseaux euclidiens.

Définition 4.1. Le **dual** d'un réseau $\mathscr{L} \subset \mathbb{R}^n$ est $\mathscr{L}^\vee := \{x \in \mathbb{R}^n \text{ tel que } \forall y \in \mathscr{L}, \langle x, y\rangle \in \mathbb{Z}\}$.

Un réseau étant défini par sa base, on va pouvoir définir le dual d'un réseau par le dual de sa base.

Définition 4.2. Soit $(b_i)_{1\leq i\leq m}$ une base de $\mathbb{R}^m$, on définit sa **base duale** $(b_i^\vee)_{1\leq i\leq m}$ par les relations suivantes :

$$\langle b_i^\vee, b_j\rangle = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$$

Proposition 4.1. Soit $\mathbf{B}$ la matrice de la base, soit D la matrice de la base duale associée à B.

— on a $D = B^{-t}$ lorsque le réseau est de rang plein.
— Si L n'est pas de rang plein, on a $D = B(B^tB)^{-1}$.
— Le dual du dual est la base de départ.

Proposition 4.2. On a $\mathscr{L} = \mathscr{L}(b_1, \cdots, b_m)$ si et seulement si $\mathscr{L}^\vee = \mathscr{L}(b_1^\vee, \cdots, b_n^\vee)$

Proposition 4.3. Soit $\mathscr{L}$ un réseau.

— $\text{rang}(\mathscr{L}) = \text{rang}(\mathscr{L}^\vee)$.
— $det(\mathscr{L}^\vee) = \det(\mathscr{L})^{-1}$.

Proposition 4.4. Soit $\mathscr{L}$ un réseau.

— pour tout $a \in \mathbb{R}^*$, on a $(a\mathscr{L})^\vee = \frac{1}{a}\mathscr{L}^\vee$.
— si $\mathscr{L} = \mathbb{Z}u$ pour $u \in \mathbb{R}^m$, alors $\mathscr{L}^\vee = \frac{1}{\|u\|^2}\mathbb{Z}u$.

Exemple. Le réseau dual de $\mathbb{Z}^n$ est $\mathbb{Z}^n$.

Proposition 4.5. Soit $\mathscr{L}_1$, $\mathscr{L}_2$ des réseaux, $(\mathscr{L}_1 \oplus \mathscr{L}_2)^\vee = \mathscr{L}_1^\vee \oplus \mathscr{L}_2^\vee$

4.1 Quelques réseaux usuels

Définition 4.3. On définit le réseau euclidien $A_n \subset \mathbb{R}^{n+1}$ par :

$$A_n = \left\{ (x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} \;\middle|\; \sum_{i=1}^{n+1} x_i = 0 \right\}$$

Exemple. On a :

$$\begin{aligned}
&A_0 = \{0\} \subset \mathbb{R},\\
&A_1 = \{(x,-x) \in \mathbb{Z}^2\}, \text{ donc } A_1 \text{ est de rang } 1\\
&A_2 = \{(x,y,z) \in \mathbb{Z}^3 \mid x+y+z=0\},\\
&\quad = \langle a_1, a_2\rangle \quad \text{où } a_1 = (1,-1,0), \quad a_2 = (0,1,-1),\\
&\quad \text{donc } A_2 \text{ est de rang } 2.
\end{aligned}$$

Proposition 4.6. Pour tout $n \in \mathbb{N}$, A_n a pour matrice génératrice :

$$B_n := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0\\ -1 & 1 & 0 & \cdots & 0\\ 0 & -1 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ 0 & 0 & \cdots & -1 & 1 \end{pmatrix} \in M_n(\mathbb{Z})$$

Proposition 4.7. A_n est un réseau euclidien de rang n, pour tout $n \in \mathbb{N}$.

Conclusion et perspectives

ANNEXE **A**

Rappels d'algèbre : Groupes, Anneaux et Modules

A.1 Groupes

ANNEXE **B**

Rappels sur les anneaux

B.1 Généralités

Ces résultats sont classiques de la théorie des anneaux commutatifs. Pour plus de détails, on pourra se reporter à un manuel standard d'algèbre.

Définition B.1. Un **anneau** $(A, +, \cdot)$ est un ensemble A muni de deux lois internes :

— $(A, +)$ est un **groupe abélien** (on note 0 son élément neutre et $-a$ l'inverse de a),

— la multiplication $\cdot : A \times A \to A$, notée simplement ab, est **associative** et **distributive** par rapport à $+$, c'est-à-dire :

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca, \quad \forall a, b, c \in A,$$

et possède un **élément neutre** $1 \in A$ (on dit alors que A est un anneau **unitaire**).

Définition B.2. Un anneau A est **commutatif** si $ab = ba$ pour tout $a, b \in A$.

Dans ce mémoire et dans cette annexe, tous les anneaux seront supposés commutatifs par défaut, conformément aux usages standards, sauf indication explicite du contraire.

Définition B.3. Un anneau A est **intègre** si, pour tout $a, b \in A$, on a

$$ab = 0 \quad \Longrightarrow \quad (a = 0 \text{ ou } b = 0).$$

Remarque. Autrement dit, A est intègre si et seulement si il n'a pas de diviseurs de 0.

Définition B.4. Soit A un anneau commutatif. Un **idéal** $I \subseteq A$ est un sous-groupe additif de $(A, +)$ tel que, pour tout $a \in A$ et tout $x \in I$, on ait $ax \in I$.

Remarque. En commutatif, $ax = xa$, donc une seule condition suffit à le décrire.

Définition B.5. Un idéal I de A est dit **principal** s'il existe un unique $r \in A$ tel que $I = \langle r \rangle = \{ar : a \in A\}$. Un anneau A est **principal** si tous ses idéaux sont principaux.

Définition B.6. Un anneau A est **noethérien** si toutes ses chaînes d'idéaux (i.e. $I_1 \subseteq I_2 \subseteq \ldots$) sont stationnaires, c'est-à-dire qu'il n'existe pas de chaîne infinie strictement croissante d'idéaux.

Remarque. Cette définition est équivalente à dire que tout idéal de A est de type fini, i.e. $I = \langle x_1, \ldots, x_k \rangle$ pour un nombre fini d'éléments.

Définition B.7 (Anneau factoriel)**.** Un anneau intègre A est **factoriel** si tout élément non nul et non inversible de A admet une factorisation en éléments irréductibles unique à l'ordre près (et inversibles près).

Tout **anneau euclidien** est principal, tout **anneau principal** est factoriel et tout **anneau principal** est noethérien.

TABLE B.1 – Quelques exemples d'anneaux et leurs propriétés

Anneau	Commutatif	Intègre	Principal	Factoriel	Noethérien
$\mathbb{Z}$	✓	✓	✓	✓	✓
$\mathbb{Z}/n\mathbb{Z}$ (non premier)	✓	✗	✓	✗	✓
$\mathbb{Z}/p\mathbb{Z}$ (p premier)	✓	✓	✓	✓	✓
$\mathbb{Z}[i]$	✓	✓	✓	✓	✓
$\mathbb{Z}[\sqrt{-5}]$	✓	✓	✗	✗	✓
$\mathbb{Z} \times \mathbb{Z}$	✓	✗	✗	✗	✓
$M_n(\mathbb{K})$, $n \geq 2$	✗	✗	—	—	✓
$C^0([0,1], \mathbb{R})$	✓	✓	✗	✗	✗

B.2 Anneaux de polynômes

Les matrices polynomiales que nous étudierons dans ce mémoire sont construites à partir d'anneaux de polynômes, qui en forment la base algébrique.

Théorème B.1. Si A est un anneau factoriel, alors $A[x]$ est aussi factoriel.
Si A est un anneau noethérien, alors $A[x]$ est noethérien.
Si A est intègre, alors $A[x]$ est intègre.

Proposition B.1. Soit $\mathbb{K}$ un corps. Alors l'anneau de polynômes $\mathbb{K}[x]$ est **principal** et l'anneau $\mathbb{K}[x, y]$ **n'est pas** principal.

Remarque. Quand on a deux variables, la structure d'idéaux se complique et ne peut pas être engendrée par un seul polynôme dans la plupart des cas.

TABLE B.2 – Exemples d'anneaux de polynômes et leurs propriétés

Anneau	Commutatif	Intègre	Principal	Factoriel	Noethérien
$\mathbb{K}[x]$	✓	✓	✓	✓	✓
$\mathbb{K}[x, y]$	✓	✓	✗	✓	✓
$\mathbb{Z}[x]$	✓	✓	✗	✓	✓
$\mathbb{F}_p[x]$	✓	✓	✓	✓	✓
$\mathbb{F}_p[x, y]$	✓	✓	✗	✓	✓
$\mathbb{R}[x]/(x^2+1)$	✓	✓	✓	✓	✓
$\mathbb{K}[x]/(x^n)$, $n \geq 2$	✓	✗	✓	✗	✓

ANNEXE C

Rappels sur les modules

C.1 Généralités

Définition C.1. Soit A un anneau commutatif unitaire. Un **A-module** $(M, +, \cdot)$ est un ensemble M :

— muni d'une loi interne $+$ faisant de $(M, +)$ un groupe abélien,

— muni d'une loi externe $A \times M \to M,\ (a, m) \mapsto am$, satisfaisant pour tout $a, b \in A$ et $m, m' \in M$:

1. Distributivité : $a(m + m') = am + am'$,
2. Distributivité : $(a + b)m = am + bm$,
3. Associativité : $(ab)m = a(bm)$,
4. Neutre : $1 \cdot m = m$ (où 1 est l'élément neutre de A).

Remarque. Cette définition généralise la notion d'espace vectoriel, en remplaçant le *corps* des scalaires par un *anneau* commutatif. Dans le cas d'un corps, tout élément non nul de A est inversible, tandis qu'ici on n'exige pas cette propriété.

Exemple. Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{Z}^n$, muni de l'addition vectorielle et de la multiplication par un scalaire entier, est un $\mathbb{Z}$-module. En effet :

— $(\mathbb{Z}^n, +)$ est un groupe abélien,

— pour tout $a \in \mathbb{Z}$ et $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, on a $a \cdot x = (ax_1, \ldots, ax_n) \in \mathbb{Z}^n$,

— toutes les axiomes d'un module sont satisfaits (associativité, distributivité, existence d'un neutre).

C'est un module libre de type fini, de base canonique $(e_1, \ldots, e_n)$.

Contre exemple. Considérons l'ensemble $\mathbb{R}$ et l'anneau $\mathbb{C}$. On cherche à définir une structure de $\mathbb{C}$-module sur $\mathbb{R}$ via la multiplication usuelle :

$$\forall \alpha \in \mathbb{C},\ \forall r \in \mathbb{R}, \quad \alpha \cdot r := \alpha r.$$

Cependant, cette loi externe n'est pas bien définie car elle n'est pas **fermée** :

$$\text{par exemple, } \alpha = i \in \mathbb{C},\ r = 1 \in \mathbb{R} \quad \Rightarrow \quad \alpha \cdot r = i \notin \mathbb{R}.$$

Donc $\mathbb{R}$ n'est pas stable par multiplication par les scalaires complexes. Il ne peut pas être muni d'une structure de $\mathbb{C}$-module.

C.1.1 Sous-modules, type fini et modules libres

Définition C.2. Soit M un A-module. Un **sous-module** $N \subseteq M$ est un sous-groupe additif de $(M, +)$ qui est stable par multiplication externe, c'est-à-dire pour tout $a \in A$ et tout $x \in N$, on a $ax \in N$.

TABLE C.1 – Exemples et contre-exemples de modules

Ensemble considéré	**Sur quel anneau A**	**Module ?**
$\mathbb{Z}^n$	$\mathbb{Z}$	✓
$\mathbb{Q}^n$	$\mathbb{Q}$	✓
$\mathbb{Z}/n\mathbb{Z}$	$\mathbb{Z}$	✓
$C^0([0,1],\mathbb{R})$	$\mathbb{R}$	✓
$\mathbb{R}[x]$	$\mathbb{R}$	✓
$\mathbb{Q}$	$\mathbb{Z}$	✗
$\mathbb{Z}[\sqrt{2}]$	$\mathbb{Z}[x]$	✗
$\mathbb{R}$	$\mathbb{C}$	✗
$\mathbb{Z}^n$	$\mathbb{Q}$	✗

Définition C.3. Un A-module M est de **type fini** s'il existe un ensemble fini $S \subset M$ tel que tout élément de M s'écrive comme combinaison A-linéaire des éléments de S. On dit alors que S engendre M.

Définition C.4. Un A-module M est **libre** s'il admet une famille $(x_i)_{i\in I}$ telle que tout $x \in M$ s'écrive de manière unique sous la forme

$$x \;=\; \sum_{i\in I} \alpha_i \, x_i,$$

avec $\alpha_i \in A$. Cette famille (x_i) est appelée **base** de M.

Si M est libre et de type fini, il existe donc une base finie de M. La démonstration n'est pas triviale. Dans ce cas, toutes les bases de M ont le même nombre d'éléments, que l'on appelle le **rang** de M.

Exemple. .

— $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module de type fini, mais il n'est pas libre pour $n \neq 0$, car aucun élément non nul de $\mathbb{Z}/n\mathbb{Z}$ n'est librement générateur.

— Au contraire, $\mathbb{Z}^n$ est libre de rang n (les vecteurs de la base canonique en constituent une base).

Libre	**Type fini**	**Exemple**
Oui	Oui	$\mathbb{Z}^n$
Oui	Non	$\bigoplus_{i\in\mathbb{N}} \mathbb{Z}$
Non	Oui	$\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 2$
Non	Non	$\mathbb{Q}$

TABLE C.2 – Exemples de $\mathbb{Z}$-modules selon leur liberté et leur type fini

C.2 Modules sur un anneau principal

Dans la suite, on considère un anneau principal A, c'est-à-dire un anneau (commutatif unitaire) dans lequel *tout idéal* est principal.

Théorème C.1. Soit M un module **libre** sur un anneau principal A. Alors tout sous-module de M est également libre et son rang est inférieur ou égal à celui de M.

Exemple. Dans le $\mathbb{Z}$-module libre $\mathbb{Z}^2$, considérons le sous-ensemble

$$N \;=\; \{(a,b) \in \mathbb{Z}^2 \mid a \equiv b \pmod{10}\}.$$

On constate que N est un **sous-module** de $\mathbb{Z}^2$, et qu'il est engendré par les vecteurs $(1,1)$ et $(0,10)$. Ceux-ci sont A-linéairement indépendants, donc N est libre de rang 2, tout comme $\mathbb{Z}^2$ lui-même.

Module M	**Anneau** A	**Libre**	**Type fini**	**Torsion**	**Réf.**
$\mathbb{K}[x]^n$	$\mathbb{K}[x]$	Oui	Oui	Non	(1)
$\mathbb{K}[x]/(x^n)$	$\mathbb{K}[x]$	Non	Oui	Oui	(2)
$\mathbb{K}[x]^\infty$	$\mathbb{K}[x]$	Oui	Non	Non	(3)
$\mathbb{K}(x)$	$\mathbb{K}[x]$	Non	Non	Oui	(4)
$(\mathbb{K}[x])^n/(x \cdot \mathbb{K}[x])^n$	$\mathbb{K}[x]$	Non	Oui	Oui	(5)

TABLE C.3 – Exemples de modules sur l'anneau $\mathbb{K}[x]$

Commentaires sur les exemples :

1. $\mathbb{K}[x]^n$ est le module libre canonique : c'est un $\mathbb{K}[x]$-module libre de rang n. Il sert de modèle aux réseaux polynomiaux.
2. $\mathbb{K}[x]/(x^n)$ est un module de torsion : tout élément est annulé par une puissance de x. Il n'admet pas de base libre.
3. $\mathbb{K}[x]^\infty$ (somme directe infinie) est un module libre, mais non de type fini. Il possède une base infinie indexée par $\mathbb{N}$.
4. $\mathbb{K}(x)$, le corps des fractions rationnelles, est un module divisible mais non libre. Il contient des éléments sans expression unique comme combinaison de base.
5. $(\mathbb{K}[x])^n/(x\cdot\mathbb{K}[x])^n$ est un module quotient, utilisé dans les algorithmes de bases d'ordre modulo x^σ. C'est un module de torsion.

ANNEXE D

Rappels d'algèbre linéaire

Dans ce mémoire, on se place dans l'espace euclidien $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$, muni du produit scalaire canonique et de la norme euclidienne associée $\| \cdot \|_2$.

Définition D.1. Soient $n, p \in \mathbb{N}^*$, $1 \leq i \leq n$ et $1 \leq j \leq p$.
On définit la **matrice élémentaire** $E_{i,j} \in M^{n \times p}(\mathbb{K})$ par :

$$E_{i,j} = (\delta_{k,i}\delta_{l,j})_{1 \leq k \leq n,\ 1 \leq l \leq p},$$

où δ désigne le *symbole de Kronecker*.

D.1 Orthonormalisation de Gram–Schmidt (GSO)

Définition D.2 (Base orthogonale)**.** Une base $(b_i)_{1 \leq i \leq n}$ de $\mathbb{R}^n$ est dite **orthogonale** si

$$\langle b_i, b_j \rangle = 0 \quad \text{pour tout } i \neq j.$$

Soit $B = (b_1, \ldots, b_n)$ une base de $\mathbb{R}^n$. On construit une base orthogonale associée $B^* = (b_1^*, \ldots, b_n^*)$ de la façon suivante, appelée **procédé d'orthogonalisation de Gram-Schmidt** :

$$b_1^* \coloneqq b_1, \quad b_i^* \coloneqq b_i - \sum_{j=1}^{i-1} \mu_{i,j}\, b_j^*, \quad \mu_{i,j} \coloneqq \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}.$$

Les coefficients $\mu_{i,j}$ sont appelés **coefficients de Gram-Schmidt**. Si on note B^* la matrice dont les lignes sont les b_i^* et

$$U = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \mu_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \mu_{n,1} & \cdots & \mu_{n,n-1} & 1 \end{pmatrix},$$

alors on a

$$B = U\, B^* \tag{D.1}$$

Remarque.

- U est triangulaire inférieure, avec $\det(U) = 1$.
- Nous n'effectuons pas de normalisation, afin d'éviter l'introduction de racines irrationnelles et de conserver l'information volumétrique du réseau associé.

Proposition D.1. La famille $(b_i^*)_{1 \leq i \leq n}$ obtenue est orthogonale.

Preuve. Pour $n = 1$, la famille est clairement orthogonale.

Supposons que $(b_i^*)_{1\leq i\leq k}$ est orthogonale.
Alors

$$\begin{aligned}\left\langle b_{k+1}^*, b_i^*\right\rangle &= \left\langle b_{k+1} - \sum_{j=1}^{k} \frac{\left\langle b_{k+1}, b_j^*\right\rangle}{\left\|b_j^*\right\|^2} b_j^*, b_i^* \right\rangle \\ &= \langle b_{k+1}, b_i^*\rangle - \left\langle \sum_{j=1}^{k} \frac{\left\langle b_{k+1}, b_j^*\right\rangle}{\left\|b_j^*\right\|^2} b_j^*, b_i^* \right\rangle \\ &= \langle b_{k+1}, b_i^*\rangle - \left\langle \frac{\left\langle b_{k+1}, b_i^*\right\rangle}{\left\|b_i^*\right\|^2} b_i^*, b_i^* \right\rangle = 0\end{aligned}$$

donc la famille $(b_i^*)_{1\leq i\leq k+1}$ est orthogonale et par le procédé de récurrence la famille $(b_i^*)_{1\leq i\leq n}$ est orthogonale. ■

Proposition D.2. On $\operatorname{adet}(B) = \det(B^*) = \prod_{i=1}^{n} \|b_i^*\|$.

Preuve. $\det(B) = \det(UB^*) \overset{(D.1)}{=} \det(U)\det(B^*) = \det(B^*) \overset{(1.3)}{=} \prod_{i=1}^{n} \|b_i^*\|$ ■

Définition D.3. Le **complément orthogonal** de U, que l'on dénote par $U^\perp$, est défini par

$$\{x \in V \mid \langle x, \mathbf{d}\rangle = 0 \quad \forall\, d \in U\}.$$

Proposition D.3. g_k^* est la projection de g_k sur le complément orthogonal $\left(\sum_{1\leq i<k} \mathbb{R}g_i\right)^\perp$

Algorithme 10 : *Orthogonalisation de Gram–Schmidt*

Entrée : Une base $B = (b_1, \ldots, b_n)$
Sortie : La base orthogonale $B^* = (b_1^*, \ldots, b_n^*)$ et la matrice U des coefficients de Gram–Schmidt

```
1 for k = 1 to n do
2     b_k^* ← b_k;
3     for j = 1 to k − 1 do
4         U_{k,j} ← ⟨b_k^*, b_j^*⟩ / ‖b_j^*‖²;
5         b_k^* ← b_k^* − U_{k,j} b_j^*;
```

Théorème D.1. L'algorithme *Orthogonalisation de Gram-Schmidt* effectue au plus $\mathcal{O}(n^3)$ opérations arithmétiques dans $\mathbb{Q}$.

D.2 Matrice de Gram

Définition D.4. La **matrice de Gram** associée à la famille $(e_1, \ldots, e_n)$ est la matrice

$$G \;=\; \big(\langle e_i, e_j\rangle\big)_{1\leq i,j\leq n}.$$

Remarque.

- Les éléments diagonaux de G sont les carrés des normes $\|e_i\|^2$.
- Les éléments hors diagonale mesurent l'orientation relative entre les vecteurs, via $\langle e_i, e_j \rangle$.
- G est une matrice symétrique réelle.

Rappelons enfin que si u et v sont des vecteurs unitaires, alors $\langle u, v \rangle = \cos(\theta)$, où θ est l'angle entre u et v. Ainsi :

- $\langle u, v \rangle = 1$ signifie que u et v sont alignés et de même sens,
- $\langle u, v \rangle = 0$ signifie que u et v sont orthogonaux,
- $\langle u, v \rangle = -1$ signifie que u et v sont alignés, mais de sens opposé.

Ce point de vue fait de la matrice de Gram un outil privilégié pour évaluer la similarité directionnelle dans un ensemble de vecteurs.

Bibliographie

AJTAI, M. (1996). « Generating hard instances of lattice problems (extended abstract) ». In : *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. STOC '96. ACM Press, p. 99-108. DOI : 10.1145/237814.237838. URL : http://dx.doi.org/10.1145/237814.237838.

BOSTAN, Alin et Éric SCHOST (août 2005). « Polynomial evaluation and interpolation on special sets of points ». In : *Journal of Complexity* 21.4, p. 420-446. ISSN : 0885-064X. DOI : 10.1016/j.jco.2004.09.009. URL : http://dx.doi.org/10.1016/j.jco.2004.09.009.

MULDERS, T. et A. STORJOHANN (avr. 2003). « On lattice reduction for polynomial matrices ». In : *Journal of Symbolic Computation* 35.4, p. 377-401. ISSN : 0747-7171. DOI : 10.1016/s0747-7171(02)00139-6. URL : http://dx.doi.org/10.1016/S0747-7171(02)00139-6.