Rapport de stage

Réduction de réseaux - adaptations d'idées provenant du cas polynomiale au cas entier.

HAI001I : Stage académique

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

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

Date : 17 février - 26 juin 2025

Table des matières

Notations **2**

Guide de Lecture **3**

1 Réseaux euclidiens et polynomiaux **5**
1.1 Généralités sur les réseaux 5
1.1.1 Définitions et exemples 5
1.1.2 Quelques problèmes algorithmiques liés aux réseaux euclidiens 6
1.2 Réduction de réseaux euclidiens et polynomiaux 7
1.2.1 Réduction de réseaux euclidiens 7
1.2.2 Réduction de réseaux polynomiaux 7

2 Adaptation de la réduction de réseaux polynomiaux au cas entier **9**

3 Réseaux définis par relations plutôt que par générateurs **10**

A Rappels d'algèbre : Groupes, Anneaux et Modules **12**
A.1 Définition et propriétés des groupes 12
A.2 Définition et propriétés des anneaux 12
A.2.1 Généralités 12
A.2.2 Anneaux de polynômes 13
A.3 Définition et propriétés des modules 13
A.3.1 Généralités 13
A.3.2 Modules sur un anneau principal 14

B Rappels d'algèbre linéaire **15**
B.1 Orthonormalisation de Gram-Schmidt (GSO) 15

C Code SageMath **16**

Notations

Cette section est conçue comme un lexique dans lequel sont répertorié les notations de ce mémoire.

$\mathbb{Z}$: L'ensemble des entiers relatifs.

$\mathbb{R}$: L'ensemble des réels.

$\mathcal{L}$: Un réseau, désigné par une lettre majuscule calligraphiée.

$\mathcal{L}(B)$ le réseau engendré par la matrice B.

A^T : La transposée de la matrice A.

$\mathbb{K}$: Un corps quelconque.

$\mathbb{F}$: Un corps fini.

$\mathbb{F}[X]$: L'anneau des polynômes univariés à coefficients dans le corps fini F.

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 les 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 où une définition est applicable et celles où elle ne l'est pas, afin de renforcer la compréhension approfondie des théorèmes et des constructions présentés.

Introduction

L'OBJECTIF de ce stage est d'explorer les réseaux euclidiens et polynomiaux, ainsi que d'analyser les techniques de réduction de réseau. L'enjeu est d'adapter les méthodes de réduction utilisées dans le cadre des réseaux polynomiaux au cas des réseaux entiers.

La réduction de réseau est un outil essentiel dans plusieurs domaines de la cryptographie, notamment dans les algorithmes de sécurité basés sur la difficulté de résoudre des problèmes liés aux réseaux. En particulier, la réduction de réseaux polynomiaux est connue de manière polynomiale, et l'adaptation de ces méthodes pour les réseaux entiers pourrait avoir des implications importantes pour la sécurité des systèmes cryptographiques. Ce stage vise donc à approfondir cette adaptation et à en étudier les applications pratiques.

CHAPITRE 1

Réseaux euclidiens et polynomiaux

L'ÉTUDE des réseaux euclidiens en mathématiques trouve ses origines au XVIIIe siècle, lorsque Leonhard Euler a exploré les structures géométriques des points dans l'espace. Toutefois, ce n'est que dans le courant du XXe siècle que le concept de réseaux euclidiens a été intégré à la cryptographie. Dans les années 1990, des chercheurs tels qu'Ajtai, Dwork, Regev et d'autres ont introduit l'idée des réseaux euclidiens comme fondement de problèmes complexes en cryptographie, ouvrant ainsi la voie à de nouvelles constructions cryptographiques.

1.1 Généralités sur les réseaux

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 $\langle f, g \rangle$. Ici, nous utiliserons le produit scalaire usuel, défini par $\langle f, g \rangle = f \cdot g^T$ lequel induit la norme-2, donnée par $\|f\|_2 = (f \cdot f^T)^{1/2}$.

Dans la littérature, on trouve les trois définitions suivantes d'un réseau euclidien qui représentent le même objet.

Définition 1.1 (GATHEN et GERHARD 2003)**.** Soit $n \in \mathbb{N}$ et $f_1, \cdots, f_n \in \mathbb{R}^n$.
Alors $\mathcal{L} = \sum_{1 \leq i \leq n} \mathbb{Z} f_i$ est un réseau euclidien

Définition 1.2 (WALLET s. d.)**.** Un **réseau euclidien** est un sous-groupe discret de $\mathbb{R}^n$

Définition 1.3 (ALLINI 2014)**.** Un **réseau euclidien** (Λ, q) est un $\mathbb{Z}$-module libre Λ de rang fini avec une forme quadratique définie positive q sur $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$

Soit $\mathcal{L}$ un réseau euclidien. Il existe une famille $\mathbb{Z}$-libre maximale $(b_i)_{1 \leq i \leq n}$ dans $\mathcal{L}$ tel que $\mathcal{L} = Zb_1 \oplus \cdots \oplus Zb_n$, qu'on appelle **base du réseau** $\mathcal{L}$, si on note B la matrice des (b_i) on notera $L(B)$ le réseau de base B, donc engendré par les (b_i).

L'entier n est commun à toutes les bases de L et on l'appelle rang de L. Lorsque $n = m$, on dit que le réseau est de rang plein.

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

Définition 1.4. La taille d'un réseau $L(B)$ est $det(B)$ et est noté $\|L\|$. La taille d'un réseau est indépendant de la base choisie.

En substituant $\mathbb{Z}$ par un anneau de polynômes, on obtient ce qu'on appelle les réseaux polynomiaux.

Exemple 1.1.

Définition 1.5 (WALLET s. d.)**.** On appelle **minimum d'un réseau** $\mathcal{L}$ la quantité

$$\lambda_1 = min\{r > 0 : |\mathcal{B}(r) \cap \mathcal{L}| > 1\} \in \mathbb{R}_+$$

On a vu que différentes bases peuvent être associées à un même réseau. Existe-t-il une notion de "bonne base" ? Nous verrons qu'une base idéale est celle qui est la plus orthogonale possible. Cette question est en lien avec des problèmes ouverts majeurs, tels que leShortest Vector Problem (SVP) et le closest vector problem (CVP).

Exemple 1.2. 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 on voit que $det(U) = -1$. Donc B et B' engendrent le même réseau $\mathcal{L}$.

On a $\|L\| = 1$ et $\lambda_1(\mathcal{L}) = 1$

1.1.2 Quelques problèmes algorithmiques liés aux réseaux euclidiens

Le calcul du plus court vecteur dans un réseau est un problème difficile.
Considérons le problème suivant :

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

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

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

L'état des connaissances actuelles est le suivant :

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

Un autre problème important concerne la recherche de vecteurs proches dans un réseau.

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

$$\|t - v\| = d(t, L) := \min\{\|t - v\| \mid v \in L\}.$$

De même, on peut considérer une version approximative :

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

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

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.

1.2 Réduction de réseaux euclidiens et polynomiaux

La réduction de réseaux est un outil fondamental en cryptographie et, plus généralement, en calcul formel. La réduction d'un réseau consiste à modifier une base quelconque de ce réseau en une base presque orthogonale. L'intérêt est de trouver de "bonnes" bases afin de résoudre divers problèmes.

Nous avons deux résultats distincts concernant la réduction de réseaux euclidiens et polynomiaux :

— La réduction de réseaux sur $\mathbb{F}[X]$ s'effectue en temps polynomial.

— La réduction de réseaux sur $\mathbb{Z}$ est NP-difficile.

1.2.1 Réduction de réseaux euclidiens

Généralités

parler de notion de base réduite

LLL

1.2.2 Réduction de réseaux polynomiaux

Cette section sur la réduction des réseaux polynomiaux est fortement inspirée de LEBRETON 2014.

La réduction des réseaux polynomiaux est un outil essentiel. Par exemple, elle peut être utilisée pour le décodage des codes de Reed-Solomon. Dans cette partie, nous présenterons les idées et les outils permettant de réduire les réseaux polynomiaux en temps polynomial, en nous appuyant sur les meilleurs exposants connus à ce jour.

Lorsque l'on travaille avec des matrices à coefficients dans un corps fini $\mathbb{F}$, de nombreuses opérations ont des complexités équivalentes : la multiplication de matrices, l'inversion d'une matrice, le calcul du déterminant ou encore la résolution d'un système linéaire. Mais qu'en est-il lorsque les matrices ont leurs coefficients dans $\mathbb{F}[X]$?

Dans ce cas, le calcul du déterminant est équivalent à la multiplication de matrices. D'autres opérations, comme l'ordonnancement des bases et la réduction de colonnes, restent également de complexité comparable. En revanche, l'inversion d'une matrice ne l'est plus, en raison de la taille de la sortie.

La base d'ordre est un concept imortant en travaillant avec les matrices polynomiales pour réduire beaucoup de problemes à la multiplicatiob

Soit F un corps fii, F X <=d les polyonme sur F de degré <= d et F x m n les matrices m n avex coeff polynomiau

slide 6

Soit $F \in \mathbb{F}[X]^{m \times n}$. On définit $(F, \sigma) := \{v \in \mathbb{F}^{1 \times m} \text{ tel que } vF = 0 \bmod x^\sigma\}$

Proposition 1.2. (F, σ) est un $\mathbb{F}[X]$ module de dimension m.

preuve : Il faut montrer que c'est un sous-groupe additif stable pour la multiplication ?

Définition 1.6. Une base d'ordre P de F σ est une base du F X module de F σ de degré minimale

mais qsuelle est la notionn de dégré, quelle ets la notion d'ordre et de miniaité ?

Définition 1.7 (**clef_unique_0**). Soit $\mathbb{K}$ un corps et $M \in \mathbb{K}[x]_{1\times n}$. On définit le **degré de ligne** du vecteur ligne M par :

$$rdeg(M) = max(deg(m_i))_{i\in\{1,\cdots,n\}}$$

Définition 1.8 (**clef_unique_0**). Soit $\mathbb{K}$ un corps et $M \in \mathbb{K}[x]_{n\times n}$. On définit le **degré de ligne** de la matrice M par :

$$rdeg(M) = max(rdeg(ligne_i))_{i\in\{1,\cdots,n\}}$$

Exemple 1.3. Soit $M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & x+1 & 0 \\ 1 & x^3+x^2 & x & 0 \\ x^2 & 0 & x^4+x^3 & 0 \end{pmatrix} \in \mathbb{F}_2[x]$ alors $row\_degree(M) = \begin{pmatrix} 0 & 1 & 3 & 4 \end{pmatrix} \in \mathbb{Z}^4$

Mais on a un problème

Définition 1.9. Soit $s \in \mathbb{Z}^n$. On définit le degré de ligne décalé du vecteur ligne M par :

$$rdeg_s(M) = max(deg(m_i) + s_i)$$

degré décalé d'une matrice
exemple
notation x^s
remarque 2
transitivité slide 12
On va définir un ordre sur les row degree
matrice row reduced def
pour parler d'un minimum faudrait un ordre total
algo DAC je cite ALLINI 2014 et puis WIKIPEDIA CONTRIBUTORS s. d.(b) et finalement **clef_unique_4**

CHAPITRE **2**

Adaptation de la réduction de réseaux polynomiaux au cas entier

CHAPITRE 3

Réseaux définis par relations plutôt que par générateurs

Conclusion et perspectives

CHAPITRE **A**

Rappels d'algèbre : Groupes, Anneaux et Modules

A.1 Définition et propriétés des groupes

subsection Généralités
definition
exemple contre exemple

A.2 Définition et propriétés des anneaux

A.2.1 Généralités

Définition A.1. Un **anneau** $(A, +, \cdot)$ est un ensemble :

— muni d'une loi interne $+$ tel que $(M, +)$ est un groupe abélien.

— muni d'une loi interne $A \times A \to A, (a, b) \mapsto a \cdot b$ qu'on notera ab vérifiant les trois propriétés suivantes :

1. $\cdot$ distributif sur $+$:
   — $a(b + c) = ab + ac$
   — $(b + c)a = ba + ca$
2. $\cdot$ est associatif
3. $\cdot$ a un élément neutre

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

Définition A.3. Un anneau A est **intègre** si $ab = 0 \Rightarrow a = 0$ ou $b = 0$ pour tout $a, b \in A$

Définition A.4. Soit A un anneau. Un **idéal** I de A est un sous-ensemble de A tel que

1. I est un sous-groupe additif de $(A, +)$
2. pour tout $a \in A$, $x \in I$, on a $ax \in I$ et $xa \in I$

def anneau euclidien

Définition A.5. Un idéal est dit **principal** s'il est engendré par un élément. Un anneau A est dit **principal** si tous ses anneaux sont principaux.

def Anneau noetherien
prop anneau noetherien
def anneau factoriek

Théorème A.1. Tout anneau principal est factoriel.

Théorème A.2. Tout anneau euclidien est principal

Théorème A.3. Tout anneau principal est noetherien

Théorème A.4. ctout anneau commutatif intègre et principal est foactoriel

proposition des implications schéma d'inclusion récap pq pas.

A.2.2 Anneaux de polynômes

Dans ce mémoire, les anneaux de polynômes constituent un type d'anneaux particulièrement utile.

Théorème A.5. Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

Remarque A.1. Il s'en suit que $A[X, Y]$ est factoriel et ainsi de suite.

Théorème A.6. Si A est un anneau Noethérien, alors $A[X]$ est un anneau Noethérien.

Remarque A.2. Il s'en suit que $A[X, Y]$ est Noethérien et ainsi de suite.

Théorème A.7. Si A est un anneau factoriel, alors $A[X]$ est un anneau intègre.

Remarque A.3. Il s'en suit que $A[X, Y]$ est intègre et ainsi de suite.

Si K corps K X principal je crois

Proposition A.1. $K[X]$ est principal.

Proposition A.2. $K[X, Y]$ n'est pas principal.

A.3 Définition et propriétés des modules

A.3.1 Généralités

Cette partie se base sur WIKIPEDIA CONTRIBUTORS s. d.(a) et HARARI s. d.

La notion de module est la généralisation naturelle de celle d'espace vectoriel. Dans toute la suite A désigne un anneau commutatif.

Définition A.6. Un **A-module** $(M, +, \cdot)$ est un ensemble :

- muni d'une loi interne $+$ tel que $(M, +)$ est un groupe abélien.
- muni d'une loi externe $A \times M \to M, (a, m) \mapsto a \cdot m$, qu'on notera am vérifiant les quatre propriétés suivantes :
  1. Distributivité : $\alpha(m + m') = \alpha m + \alpha m'$
  2. Distributivité : $(\alpha + \beta)m = \alpha m + \beta m$

3. Associativité : $(\alpha\beta)m = \alpha(\beta m)$
4. Neutre : $1m = m$
   pour tout α, $\beta \in A$ et m, $m' \in M$

Remarque A.4. La définition d'un module peut être vue comme une généralisation de celle d'un espace vectoriel. En effet, un module est un espace vectoriel dans lequel l'hypothèse sur A est affaiblie : au lieu d'être un corps, A est un anneau, ici commutatif, on ne se soucie donc pas de la distinction entre modules à gauche ou à droite.

Exemple A.1. Soit $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module.

Définition A.7. Soit M un A-module. Un **sous-module** N de M est un sous-groupe de $(M, +)$ stable pour la multiplication externe par tout élément de A.

Définition A.8. Un A-module M est dit de **type fini** s'il existe une partie finie S de M tel que M soit engendré par S.

Définition A.9. Un A-module M est dit **libre** s'il admet une base i.e. si il admet une famille $(x_i)_{i\in I}$ tel que pour tout $x \in M$, x s'écrit de manière unique comme $\sum_{i\in I} \alpha_i x_i$

Proposition A.3. Si M est libre et de type fini, alors il admet une base finie. On dit dans ce cas que M est libre de type fini, et toutes les bases de M ont le même cardinal, qu'on appelle rang de M.

Exemple A.2. $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module de type fini mais pas libre pour $n \neq 0$.

A.3.2 Modules sur un anneau principal

Dans cette partie, A désigne un anneau principal.

Théorème A.8. Si M est un module libre sur un anneau principal A, tout sous-module de M est libre et de rang inférieur ou égal à celui de M.

Exemple A.3. Dans le $\mathbb{Z}$-module libre $\mathbb{Z}^2$, le sous-module des couples (a, b) tels que $a \equiv b$ mod 10 est libre de base $((1, 1), (0, 10))$ donc de rang 2 (comme le module lui-même).

CHAPITRE **B**

Rappels d'algèbre linéaire

B.1 Orthonormalisation de Gram-Schmidt (GSO)

On se considère dans un espace euclidien. Soit $B = (b_i)_{1 \leq i \leq n}$ une base de $\mathbb{R}^n$, on peut construire la **base de Gram-Schmidt (GS)** associée à cette base par le procédé récursif suivant :

$$b_1^* := b_1$$

$$b_i^* := b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*, \quad \text{avec } \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$$

où $\mu_{i,j}$ est appelé **coefficient de Gram-Schmidt** associé au vecteur b_i.

Notons B^* la matrice des b_i^*, et U la matrice des $\mu_{i,j}$. Alors, on a la relation :

$$B = B^* U$$

Remarque B.1. — U est triangulaire avec un déterminant égal à 1.

— On ne normalise pas, sinon cela introduit des racines et on risque de passer de $\mathbb{Q}$ à $\mathbb{R} \setminus \mathbb{Q}$. De plus, la normalisation impose un volume de 1 et ne conserve donc pas l'information volumique du réseau associé.

Proposition B.1. — Conservation du volume : $\det L = \prod \|b_i^*\|$.

— Propriété du plus petit vecteur** : $\lambda_1(\mathcal{L}) \geq \min \|b_i^*\|$.

Le coût de l'algorithme de Gram-Schmidt (GSO) est en $O(n^3)$ opérations arithmétiques dans $\mathbb{Q}$.

CHAPITRE **C**

Code SageMath

Bibliographie

ALLINI, Elie Noumon (2014). *Théorie alorithmique des nombres*. Diaporama.

GATHEN, Joachim Von Zur et Jurgen GERHARD (2003). *Modern Computer Algebra*. 2e éd. USA : Cambridge University Press. ISBN : 0521826462.

HARARI, David (s. d.). *Modules sur un anneau commutatif*.

LEBRETON, Romain (2014). *A crash course on Order Bases : Theory and Algorithms*. Diaporama.

WALLET, Alexandre (s. d.). *Réseaux euclidiens et cryptographie*. Document PDF, Notes de cours.

WIKIPEDIA CONTRIBUTORS (s. d.[a]). *Module sur un anneau*.

— (s. d.[b]). *Réseau (géométrie)*.