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

Remerciements

Table des matières

Notations

$\mathbb{Z}$ désigne l'ensemble des entiers relatifs.
$\mathbb{R}$ désigne l'ensemble des réels.
Les réseaux seront désignés par une lettre majuscule calligraphiée, telle que $\mathcal{L}$.

Guide de lecture

Introduction

L'objectif de mon stage est d'étudier les réseaux euclidiens et polynomiaux, ainsi que d'analyser les techniques de réduction de réseau afin d'adapter celles du cas polynomial au cas entier.

La réduction de réseau polynomiaux est un outil important en cryptographie

Chapitre 1

Réseaux euclidiens et polynomiaux

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 $\|f\|_2 = (f \cdot f^T)^{1/2}$.

Définition 1.1. Soit $n \in \mathbb{N}$. Z module reseau "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 $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$

Exemple 1.1.

def de la base d'un reseau
def d'un plus court vecteur

Définition 1.4 (Wallet s. d.)**.** On appelle minimum d'un réseau $\mathcal{L}$ la quantité

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

problematique -> differentes bases -> des bases avec de cours vecteurs,
parler des problemes SVP probleme NP -difficile

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.

def Orthogonalisation de Gram-Scmidt exemple parler de la complexité de Gram Schmidt

1.2 Réduction de réseaux euclidiens et polynomiaux

1.2.1 Réduction de réseaux euclidiens

1.2.2 Réduction de réseaux polynomiaux

reseau reduit chap 16

Définition 1.5 (Lebreton 2014)**.** 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 1.6 (Lebreton 2014)**.** 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 1.2. 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 $row\_degree(M) = \begin{pmatrix} 0 & 1 & 3 & 4 \end{pmatrix} \in \mathbb{Z}^4$

Définition 1.7. Soit $s \in \mathbb{Z}^n$. On définit le degré de ligne décalé du vecteur ligne M par :

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

Je cite Wallet s. d. je cite Allini 2014 et puis Wikipedia contributors Consulté en 2025 et finalement Gathen et Gerhard 2003

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

Annexe A

Rappels d'algèbre : Groupes, Anneaux et Modules

A.1 Définition et propriétés des groupes

A.2 Définition et propriétés des anneaux

A.3 Définition et propriétés des modules

A.3.1 Généralités

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

Définition A.1. 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 : $(\alpha + b)m = \alpha m + \beta m$
  3. Associativité : $(\alpha\beta)m = \alpha(\beta m)$
  4. Neutre : $1m = m$

  pour tout α, $\beta \in Ala3$ et m, $m' \in M$

Remarque A.1. 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.

Définition A.2. 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.3. type fini

Définition A.4. libre

proposition : libre et type fini => base finie
exemples et contre-exemple

A.3.2 Modules sur un anneau principal

Dans cette partie, A désigne un anneau principal.

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.

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 (Consulté en 2025). *Réseau (géométrie)*.