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, complexité et acronymes **3**

Guide de Lecture **4**

1 Réseaux euclidiens et polynomiaux **6**
1.1 Généralités sur les réseaux 6
1.1.1 Définitions et exemples 6
1.1.2 Quelques problèmes algorithmiques liés aux réseaux euclidiens 8
1.2 Réduction de réseaux euclidiens et polynomiaux 9
1.2.1 Réduction de réseaux euclidiens 9
1.2.2 Réduction de réseaux polynomiaux 9

2 Adaptation de la réduction de réseaux polynomiaux au cas entier **14**

3 Réseaux définis par relations plutôt que par générateurs **15**

A Rappels d'algèbre : Groupes, Anneaux et Modules **17**
A.1 Définition et propriétés des groupes 17
A.2 Définition et propriétés des anneaux 17
A.2.1 Généralités 17
A.2.2 Anneaux de polynômes 18
A.3 Définition et propriétés des modules 18
A.3.1 Généralités 18
A.3.2 Modules sur un anneau principal 19

B Rappels d'algèbre linéaire **20**
B.1 Orthonormalisation de Gram-Schmidt (GSO) 20

C Code SageMath **22**

Table des algorithmes

1 BasisReduction (LLL) GATHEN et GERHARD 2003 10
2 Weak-Popov 13
3 Basis 13
4 M-Basis 13
5 PM-Basis 13
6 GramSchmidt (GSO) 21

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.
$\mathcal{L}$	Un réseau, désigné par une lettre majuscule calligraphiée.
$\mathcal{L}(\mathrm{B})$	Le réseau engendré par la matrice B.
A^T	La transposée de la matrice A.
B^*	la base de Gram-Schmidt associée à B.
$\mathbb{K}$	Un corps quelconque.
$\mathbb{F}$	Un corps fini.
$\mathbb{F}[X]$	L'anneau des polynômes uni variés à coefficients dans le corps fini $\mathbb{F}$.
$\mathbb{F}_{\leq d}[X]$	les polynôme sur $\mathbb{F}$ de degré inférieur ou égal d.
$\mathbb{F}[X]^{m\times n}$	les matrices $m \times n$ à coefficients dans $\mathbb{F}[X]$.

Complexité

Multiplication dans $\mathbb{F}_{\leq d}[X]$	$M(d) = \mathcal{O}(d \log d \log\log d)$.
Multiplication dans $\mathbb{F}^{n\times n}$	$MM(n) = \mathcal{O}(n^\omega)$, où ω est l'exposant de la multiplication matricielle.
Multiplication dans $\mathbb{F}[X]^{m\times n}_{\leq d}$	$MM(n,d) = \mathcal{O}(\mathrm{MM}(n)M(d)) = \tilde{O}(n^\omega d)$.

Note : $MM(n,d)$ peut également être obtenu via une approche d'évaluation-interpolation sur une suite géométrique, ce qui permet d'améliorer certaines bornes de complexité.

Acronymes

LLL	Lenstra–Lenstra–Lovász
BKZ	Block Korkine-Zolotarev
SVP	Shortest Vector Problem
CVP	Closest Vector Problem

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. Plus précisément, il s'agit d'adapter les méthodes de réduction développées pour les réseaux polynomiaux au cas des réseaux entiers, afin d'en évaluer l'efficacité et les implications. La réduction de réseau est un outil fondamental en cryptographie, notamment dans les algorithmes de sécurité reposant sur la difficulté de résoudre certains problèmes liés aux réseaux. En particulier, la réduction des réseaux polynomiaux est bien comprise et s'effectue en temps polynomial. L'adaptation de ces techniques aux réseaux entiers pourrait donc avoir un impact significatif sur la sécurité des systèmes cryptographiques, justifiant ainsi une étude approfondie de cette transition et de ses applications pratiques. Par ailleurs, les réseaux euclidiens constituent une approche émergente en cryptographie. Aujourd'hui, la sécurité des systèmes cryptographiques repose principalement sur la difficulté de la factorisation des grands nombres premiers et du calcul de logarithmes discrets. Cependant, ces hypothèses sont menacées par les avancées de l'informatique quantique. À l'inverse, les réseaux euclidiens offrent une alternative prometteuse pour la cryptographie post-quantique, car plusieurs de leurs problèmes fondamentaux semblent résister aux attaques quantiques. Un exemple emblématique est l'algorithme de réduction de bases LLL, qui a permis de briser plusieurs schémas cryptographiques, notamment ceux fondés sur le problème du sac à dos. Pourtant, ce même algorithme joue également un rôle clé dans la conception de nouveaux protocoles sécurisés, en exploitant la complexité intrinsèque des réseaux euclidiens pour garantir la robustesse des schémas cryptographiques.

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 $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$

Exemple 1.1. Les entiers de Gauss forment un réseau dans $\mathbb{C}$ de rang 1.

Exemple 1.2. Un exemple plus exotique, $\mathbb{Z} + \sqrt{(2)}\mathbb{Z}$ est un réseau de $\mathbb{Z}$.

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

Remarque 1.1. Nous avons la suite d'inclusions suivante : $2\mathbb{Z} \subset \mathbb{Z} \subset \frac{1}{2}\mathbb{Z}$. On observe que $\text{rang}(2\mathbb{Z}) = \text{rang}(\mathbb{Z}) = \text{rang}(\frac{1}{2}\mathbb{Z})$, bien que les 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, l'inclusion et avoir le même rang ne suffisent pas à garantir l'égalité des ensembles.

Remarque 1.2. 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 ± 1 multiplié par $\|L\|$.

définition d'un sous réseau

Nous présentons maintenant deux invariants fondamentaux d'un réseau :

— La **taille du vecteur minimal** du réseau, notée $\lambda_1(\mathcal{L})$,

— Le **volume du réseau**, aussi appelé la **taille du réseau** souvent désigné par $|\mathcal{L}|$.

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

Proposition 1.2. Soit $\mathcal{L}$ un réseau de $\mathbb{R}^n$. Si $\mathcal{L}'$ est un sous réseau de $\mathcal{L}$ alors $\|\mathcal{L}'\| divise \|\mathcal{L}\|$

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

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

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

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

Différentes bases peuvent être associées à un même réseau.

Exemple 1.3. 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 $\|\mathcal{L}\| = 1$ et $\lambda_1(\mathcal{L}) = \lambda_2(\mathcal{L}) = 1$

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 le ***Shortest Vector Problem*** (SVP) et le ***closest vector problem*** (CVP).

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 $\mathcal{L}$ de $\mathbb{R}^n$, on a :

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

.

En fait, 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 $\gamma_n \leq C_n$.

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

Remarque 1.3. Comme $\|\mathcal{L}\|$ est un invariant du réseau, si on a n'importe quelle base du réseau on peut trouver une approximation de λ_1.

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 $(b_i)_{1,\cdots,n}$ est une famille orthogonale.

Une connexion intéressante entre la base de Gram-Schmidt associée à une base d'un réseau et la norme du plus court vecteur de ce réseau.

Proposition 1.3. Soit $\mathcal{L} \subset \mathbb{R}^n$ un réseau de base $f_1, \cdots, f_n$ et soit $f_1^*, \cdots, f_n^*$ sa base de GS associé.

Alors pour tout $x \in \mathcal{L} \backslash \{0\} \|x\| \geq min\{\|f_1^*\|, \cdots, \|f_n^*\|\}$

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

Définition 1.6. GATHEN et GERHARD 2003 Soit $f_1, \cdots, f_n \in \mathbb{R}^n$ une base et $f_1^*, \cdots, f_n^* \in \mathbb{R}^n$ sa base de Gram-Schmidt associée.

On dit que $(f_1, \cdots, f_n)$ est **réduite** si $\|f_i^*\|^2 \leq 2\|f_{i+1}^*\|^2$ pour $1 \leq i \leq n$

Remarque 1.4. Chaque vecteur de la base réduite a une norme au moins égale à la moitié de celle du précédent, garantissant ainsi une décroissance modérée.

notation pour l'entier le plus proche avec la partie entiere + 1/2

L'algorithme LLL (proposé par Lenstra et al. en YYYY) repose sur un principe simple : il calcule la meilleure approximation entière de la décomposition de Gram-Schmidt et réduit la base en réorganisant les vecteurs si nécessaire. Cet algorithme est décrit dans GATHEN et GERHARD 2003.

Le code complet de l'algorithme est présenté dans l'annexe C.

1.2.2 Réduction de réseaux polynomiaux

La réduction des réseaux polynomiaux est un outil essentiel. Par exemple, elle peut être utilisée pour le décodage des codes de Reed-Solomon généralisés. 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 comme la multiplication, l'inversion, 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. L'objectif de cette partie est donc d'une part de remédier à ces problèmes, mais d'autre part de faire l'état de l'art actuel sur la réduction de réseaux polynomiaux. Cette section sur la réduction des réseaux polynomiaux est fortement inspirée de LEBRETON 2014.

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

Proposition 1.4. (F, σ) est un $\mathbb{F}[X]$-module de dimension m.

Algorithm 1 BasisReduction (LLL) GATHEN et GERHARD 2003

1

Entrée : Une base $B = (f_1, \cdots, f_n)$
Sortie : Une base réduite $G = (g_1, \cdots, g_n)$ de B
for $i = 1$ **à** n **do**
    $g_i \coloneqq f_i$
end for
$(B^*, U) \coloneqq \text{GSO}(B)$
while $i \leq n$ **do**
    for $j = i-1, i-2$ **à** 1 **do**
        $g_i := gi - \lfloor \mu_{ij} \rceil g_j$
        Mettre à jour $(B^*, U) \coloneqq \text{GSO}(B)$
    end for
    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
        $i \coloneqq i + 1$
    end if
end while
Retourner $G = (g_1, \cdots, g_n)$

Preuve 1.1. contenu...

Définition 1.7. Une (F, σ) **base d'ordre** P est une base (au sens des $\mathbb{F}[X]$-modules) (F, σ) de degré minimale.

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

Définition 1.8 (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 1.9 (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 1.4. 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, si $c = bA$, alors $rdeg(c)$ n'est pas forcément lié à $rdeg(b)$ et $rdeg(A)$.

Définition 1.10. Soit $s \in \mathbb{Z}^n$. On définit le **degré de ligne décalé** du vecteur ligne M par :

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

Définition 1.11. Soit $s \in \mathbb{Z}^n$. On définit le **degré de ligne décalé** de la matrice M par :

$$rdeg_s\left(\begin{pmatrix} ligne1 \\ \vdots \\ lignem \end{pmatrix}\right) = (rdeg_s(lignei))_{i=1,\cdots,m} \in \mathbb{Z}^m$$

On note x^s par la matrice diagonale $\begin{pmatrix} x^{s_1} & & \\ & \ddots & \\ & & x^{s_n} \end{pmatrix}$

Proposition 1.5. $rdeg_s(A) = redeg(Ax^s)$

Exemple 1.5. Si $F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & x+1 & 0 \\ 1 & x^3+x^2 & x & 0 \\ x^2 & 0 & x^4+x^3 & 0 \end{pmatrix} \in \mathbb{F}_2[x]$ et $s = (1,0,0,1)$ alors

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

Proposition 1.6. $rdeg_s(A) = v = v$ ssi $rdeg(x^{-v}Ax^s) = 0$ $rdeg_s(A) \leq v <= v$ ssi $rdeg(x^{-v}Ax^s) \leq 0$

Exemple 1.6. Si $F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & x+1 & 0 \\ 1 & x^3+x^2 & x & 0 \\ x^2 & 0 & x^4+x^3 & 0 \end{pmatrix}$, $u = (1,0,0,1)$.

Alors $v = red_u(F) = (1,2,3,4)$ et

$$x^{-v}Ax^u = \begin{pmatrix} 1 & 0 & x^{-1} & 1 \\ 1 & x^{-2} & x^{-2}+x^{-1} & 0 \\ x^{-2} & x^{-1}+1 & x^{-2} & 0 \\ x^{-1} & 0 & x^{-1}+1 & 0 \end{pmatrix}$$

Proposition 1.7. transitivité des degrés de ligne décalé 14 :27, slide 12

Preuve 1.2.

On va définir un ordre sur les rowdegree, bien que non total.

Définition 1.12. Soit $u = (u_1, \cdots, u_m)$, $v = (v_1, \cdots, v_m) \in \mathbb{Z}^m$ deux degrés de ligne, on définit $\leq_{ob}$ par :

$$u \leq_{ob} v \text{ ssi } u_i \leq v_i \forall i$$

Remarque 1.5. $\leq_{ob}$ n'est pas un ordre total.

Je pense décaler ceci dans l'annexe sur les modules :

Définition 1.13. $U \in \mathbb{F}[X]^{m \times m}$ est dit **unimodulaire** si $det(U) \in F \backslash \{0\}$

Proposition 1.8. U est unimodulaire si, et seulement si, U est inversible

Proposition 1.9. Si P, Q sont deux bases de lignes du même $\mathbb{F}[X]$-module, alors il existe U unimodulaire tel que $P = UQ$

Fin d'annexe sur les modules

Définition 1.14. Soit $F \in \mathbb{F}[X]^{m \times n}$. On dit que F est réduite par ligne si pour tout U unimodulaire, on a :

$$rdeg(F) \leq_{ob} rdeg(UF)$$

pour parler d'un minimum faudrait un ordre total
On revoit enfin la définition ref de façon rigoureuse :

Définition 1.15. Une base d'ordre P est une base du F[X]-module de F sigma qui est réduite par ligne

Proposition 1.10. il existe une base réduite par ligne P de (F, sigma)

Exemple 1.7. contenu... slide 15, à programmer

slide 16 sur tentative de preuve naive
On a l'existance, mais pas l'unicité, si on veut l'unicité, on doit avoir une condition en plus : la forme de Popov.

Définition 1.16. Soit $v = rdeg_u(A)$, alors la matrice des coefficients dominants de A, noté lcoeff(A), est la partie constante de $x^{-v}Ax^s$

exemple
on revisite le lemme de transitivité
preuve de ca
généralisation : 26 :39 Lemme Si lcoeff(A) est injective (a gauche), alors A est réduite par lignre
preuve
Comment row reduire une matrice ?
On note [d] un polynôme de degré d, on définit les pivots de ligne comme l'élément de la ligne de degré maximale le plus à droite.

Définition 1.17. Une matrice W est en forme Popov faile si ses pivots ont des indices distincts.

Exemple 1.8. contenu...

Comment rendre une matrice weak popov ?on a l'algo de mulder storjohann
Une suite decrosisante de row degree doit etre stable
lien avec base de grobner
diapao 35 :05
Weak popov => row reduced
Complexité de l'algo
$O(m^3d^2)$
on va faire mieux

Théorème 1.4. contenu...

je cite ALLINI 2014 et puis WIKIPEDIA CONTRIBUTORS s. d.(b) et finalement **clef_unique_4**

Algorithm 2 Weak-Popov

2

Entrée : $A \in \mathbb{F}[X]^{m \times n}$

Sortie : La forme de Popov faible de A

1. Ajouter des multiples d'un monôme d'une ligne à une autre afin de :

— soit déplacer un pivot vers la gauche,

— soit diminuer le degré d'une ligne.

2. S'arrêter lorsque plus aucune transformation n'est possible.

Algorithm 3 Basis

3

Hello

Algorithm 4 M-Basis

4

$P_0 := Basis(Fmodx)$
for $kde1sigma - 1$ **do**
    $F' := x^{-k} P_{k-1} F$
    $M_k := Basis(F'modx)$
    $P_k := M_k P_{k-1}$
end for
Retourner $P_{\sigma-1}$

Algorithm 5 PM-Basis

5

if $\sigma = 1$ **then**
    Retourner Basis(F mod x)
else
    P_{low} := PM-Basis $(F, \lfloor \sigma/2 \rfloor)$
    Soit F' tel que $P_lowF = xF'$
    P_{high} := PM-Basis $(F', \lfloor \sigma/2 \rfloor)$
end if
Retourner $P_{high} P_{low}$

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

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.
Z^2 peut etre vu comme un Z-module (c'est un groupe abelien pour l'addition,)

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.

un sous module dans Z n est un sous groupe de Z n avec m < n on a forcément stable multiplcaiton et le citer pour dire qu'un sous groupe d'un reseau est forcement un reseau jsp si c'est uile

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).

théorie des modules sur des anneaux principaux : on a la suite d'inclusion

ANNEXE **B**

Rappels d'algèbre linéaire

Dans ce mémoire, les matrices sont considérées comme des matrices dont les éléments sont des vecteurs ligne.

def base orthogonale

B.1 Orthonormalisation de Gram-Schmidt (GSO)

On se considère dans un espace euclidien $\mathbb{R}^n$. 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, que l'on notera $B^* = (b_i^*)_{1 \leq i \leq n}$ 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 $U = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \mu_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \mu_{n,1} & \cdots & \mu_{n,n-1} & 1 \end{pmatrix}$.

Alors, on a la relation : $B = UB^*$

Remarque B.1.

— U est triangulaire avec un déterminant égal à 1.

— Contrairement à ce qui est souvent pratiqué dans la littérature, nous n'effectuons pas de normalisation, car cela introduirait des racines, ce qui pourrait entraîner un passage des coefficients $\mathbb{Q}$ à des coefficients $\mathbb{R} \setminus \mathbb{Q}$. De plus, la normalisation impose un volume égal à 1, ce qui entraîne une perte de l'information volumétrique du réseau associé.

Proposition B.1. Soit $B = (b_i)_{1 \leq i \leq n}$ une base de $\mathbb{R}^n$, et $B^* = (b_i^*)_{1 \leq i \leq n}$ sa base de Gram-Schmidt associée.

On a $det(B) = det(B^*) = \prod \|b_i^*\|$

Démonstration. Nous utilisons le fait que U est une matrice triangulaire dont les coefficients diagonaux sont égaux à 1, et que B^* est une base de vecteurs orthogonaux. Ainsi,

$$\det(B) = \det(UB^*) = \det(U)\det(B^*) = \det(B^*) = \prod \|b_i^*\|.$$

■

Algorithm 6 GramSchmidt (GSO)

6

1: **Entrée :** Une base $B = (f_1, \cdots, f_n)$
2: **Sortie :** La base de Gram-Schmidt associée $B^* = (b_1^*, \cdots, b_n^*)$ et U la matrice des coefficients de GS
3: **for** $k = 1$ **à** n **do**
4: $\quad b_k^* \coloneqq b_k$
5: $\quad$ **for** $j = 1$ **à** k **do**
6: $\quad\quad U_{kj} \coloneqq \frac{(b_k * b_j^*)}{\|b_j^*\|^2}$
7: $\quad\quad b_k^* \coloneqq U_{kj} b_j^*$
8: $\quad$ **end for**
9: **end for**

Théorème B.1. Le coût de l'algorithme Orthonormalisation de Gram-Schmidt (GSO) est de $O(n^3)$ opérations arithmétiques dans $\mathbb{Q}$.

ANNEXE C

Code SageMath

Le code source complet est également disponible sur `https://github.com/toncompte/tonrepo`. Voici le code complet de l'algorithme implémenté :

```
def Gram_Schmidt(B):
n = B.nrows()

B_star = Matrix(QQ, n, n)
U = identity_matrix(QQ, n)

B_star[0] = B[0]

for k in range(1, n):
B_star[k] = B[k]
for j in range(k):g
U[k, j] = (B[k] * B_star[j]) / (B_star[j] * B_star[j])
B_star[k] -= U[k, j]*B_star[j]
return U, B_star


```

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)*.