RÉSEAUX EUCLIDIENS EN CRYPTOGRAPHIE
TD 1 – 2023

ALEXANDRE WALLET, QUYEN NGUYEN

Exercice 1. Soit $\mathcal{L}_1, \mathcal{L}_2$ deux réseaux de $\mathbb{R}^m$. Montrer que :
— si $\mathcal{L}_1 + \mathcal{L}_2$ est un réseau, alors $\mathrm{rk}(\mathcal{L}_1 + \mathcal{L}_2) \geq \max(\mathrm{rk}\,\mathcal{L}_1, \mathrm{rk}\,\mathcal{L}_2)$;
— $\mathcal{L}_1 \cap \mathcal{L}_2$ est un réseau et $\mathrm{rk}(\mathcal{L}_1 \cap \mathcal{L}_2) \leq \min(\mathrm{rk}\,\mathcal{L}_1, \mathrm{rk}\,\mathcal{L}_2)$.
Donner des exemples où les inégalités sont atteintes, et non atteintes.

Exercice 2. (Réseaux et non-réseaux)

(1) L'ensemble $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un réseau de $\mathbb{R}$?

(2) Soit V la droite de $\mathbb{R}^2$ engendrée par $(1, \sqrt{2})$. Quel est le rang de $\mathbb{Z}^2 \cap V$? Si π désigne la projection orthogonale sur V, l'ensemble $\pi(\mathbb{Z}^2)$ est-il un réseau de $\mathbb{R}^2$?

(3) Montrer que les sous-groupes de $\mathbb{R}$ sont soit denses, soit de la forme $\alpha\mathbb{Z}$ pour $\alpha \in \mathbb{R}$.

Exercice 3 (Problèmes algorithmiques, partie 1)**.** Le but est de donner des algorithmes pour résoudre chacun des problèmes ci-dessous. On donnera la complexité en nombre d'opérations. Dans toutes les questions, on pourra toujours supposer que les réseaux sont décrits par un système générateur.

(1) *(Base)* Soit $g_1, \ldots, g_n$ une famille génératrice d'un réseau $\mathcal{L} \subset \mathbb{R}^m$. Calculer une base de $\mathcal{L}$.

(2) *(Appartenance)* Soit $v \in \mathbb{R}^m$ et $\mathcal{L}$ un réseau de $\mathbb{R}^m$. Déterminer si $v \in \mathcal{L}$ ou non.

(3) *(Sous-réseau, égalité)* Soit $\mathcal{L}, \mathcal{L}'$ deux sous-réseaux de $\mathbb{R}^m$. Déterminer si $\mathcal{L} \subset \mathcal{L}'$, $\mathcal{L}' \subset \mathcal{L}$ ou $\mathcal{L} = \mathcal{L}'$.

(4) *(Somme de réseaux)* Donner un algorithme pour calculer une base de $\mathcal{L} + \mathcal{L}'$.

Exercice 4 (Dualité, problèmes algorithmiques, partie 2)**.** Soit $\mathcal{L} \subset \mathbb{R}^m$ un réseau et V l'espace vectoriel qu'il engendre. Le dual de $\mathcal{L}$ est l'ensemble

$$\mathcal{L}^\vee = \{u \in V \ : \ \forall\, v \in \mathcal{L}, \langle u, v\rangle \in \mathbb{Z}\}.$$

(1) Montrer que $\mathcal{L}^\vee$ est un réseau de même rang que $\mathcal{L}$. Si $\mathbf{B}$ est une base de $\mathcal{L}$, donner une base de $\mathcal{L}^\vee$.

(2) Soit $\mathcal{L}_1, \mathcal{L}_2$ deux réseaux de $\mathbb{R}^m$. Montrer que $\mathcal{L}_1^{\vee\vee} = \mathcal{L}_1$, $(\mathcal{L}_1 + \mathcal{L}_2)^\vee = \mathcal{L}_1^\vee \cap \mathcal{L}_2^\vee$ et $(\mathcal{L}_1 \cap \mathcal{L}_2)^\vee = \mathcal{L}_1^\vee + \mathcal{L}_2^\vee$.

(3) Donner un algorithme pour calculer une base de $\mathcal{L}_1 \cap \mathcal{L}_2$.

Exercice 5 (Plus difficile, faire des dessins)**.** Soit $\mathcal{L}, \mathcal{L}'$ deux réseaux de même rang.

(1) Montrer que si $\mathcal{L}' \subsetneq \mathcal{L}$, alors $\det \mathcal{L}' > \det \mathcal{L}$.

(2) Plus généralement, on veut montrer que $[\mathcal{L} : \mathcal{L}'] = \frac{\det \mathcal{L}'}{\det \mathcal{L}}$.

(a) On appelle *domaine fondamental* d'une base $\mathbf{B}$ de $\mathbb{R}^n$ l'ensemble

$$\mathcal{D}_{\mathbf{B}} = \Big\{ \sum_{i \leq n} x_i \mathbf{b}_i \ : \ x_i \in [0,1) \Big\}.$$

Montrer que $\mathbb{R}^n = \bigcup_{\mathbf{u} \in \mathcal{L}} (\mathbf{u} + \mathcal{D}_{\mathbf{B}})$, où l'union est disjointe.

(b) Soit $\mathcal{D}_{\mathbf{B}}$ et $\mathcal{D}_{\mathbf{B}'}$ des domaines fondamentaux pour $\mathcal{L}$ et $\mathcal{L}'$. Montrer que pour tout $\mathbf{u} \in \mathcal{L}$, on a $\sum_{\mathbf{x} \in \mathbf{u} + \mathcal{L}'} \mathrm{Vol}\big(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{x} + \mathcal{D}_{\mathbf{B}})\big) = \mathrm{Vol}(\mathcal{D}_{\mathbf{B}})$.

(c) En déduire que $\mathcal{L}/\mathcal{L}'$ est fini, puis le résultat annoncé.

À noter : il existe une autre preuve, plus algorithmique mais moins visuelle, reposant sur le théorème de classification des groupes abéliens.

1. Solutions

1 Si $\mathcal{L}_1 + \mathcal{L}_2$ est un réseau, il contient clairement chacune des deux opérandes. On atteint par exemple l'égalité avec $\mathcal{L}_1 = 2\mathbb{Z}$ et $\mathcal{L}_2 = 3\mathbb{Z}$, dont la somme est $\mathbb{Z}$, et tous ces réseaux sont de rang 1. L'inégalité peut être stricte : prenant e_1, e_2 la base canonique de $\mathbb{R}^2$, et $\mathcal{L}_i = \mathbb{Z}e_i$, la somme est $\mathbb{Z}^2$ qui est de rang 2. Notons ensuite que l'intersection de réseaux est toujours un ensemble discret, et donc un réseau qui est contenu dans chaque membre décrivant l'intersection. Si $\mathcal{L}_2 \subset \mathcal{L}_1$, l'intersection est $\mathcal{L}_2$ et l'inégalité est atteinte. L'exemple $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ montre que le rang peut rester le même. Enfin, $\mathbb{Z}e_1 \cap \mathbb{Z}e_2 = \{0\}$, qui montre que l'inégalité peut être stricte.

2 (1) Bien que $G = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ soit un sous-groupe de $\mathbb{R}$, il n'est pas discret et n'est donc pas un réseau de $\mathbb{R}$. Pour le montrer, il "suffit" de trouver une suite de G qui tend vers 0. Une candidate est la suite de $(\sqrt{2}-1)^n$, et il suffit donc de montrer que chacun de ses termes est dans G. Comme on a $(\sqrt{2}-1)^n = \sum_{i=0}^{n} \binom{n}{i} \sqrt{2}^i (-1)^{n-i}$, il suffit de montrer que tous les $\sqrt{2}^i$ sont dans G. Si i est pair c'est immédiat, sinon $i = 2j+1$ avec j entier et on peut écrire $\sqrt{2}^i = 2^j\sqrt{2} \in G$.

(2) La pente de cette droite est irrationnelle, et elle ne contient donc aucun point dont les coordonnées sont entières. Autrement dit, $\mathbb{Z}^2 \cap V$ est le réseau trivial $\{0\}$, et le rang de l'intersection n'est pas celui "attendu" (on s'attendrait à 1). C'est un bon signal que la projection ne va pas être un réseau non plus. On calcule facilement une matrice $\mathbf{P} = \mathbf{v} \cdot (\mathbf{v}^t\mathbf{v})^{-1} \cdot \mathbf{v}^t$ pour la projection orthogonale π :

$$\mathbf{P} = \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix} \cdot \left\|(1, \sqrt{2})\right\|^2 \cdot \begin{bmatrix} 1 & \sqrt{2} \end{bmatrix} = \frac{1}{3} \cdot \begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & 2 \end{bmatrix}.$$

Ainsi, on a $3 \cdot \pi(x, y) = (x + \sqrt{2}y, \sqrt{2}x + 2y)$ pour tout $(x, y) \in \mathbb{R}^2$ et en particulier, on voit que $3 \cdot \pi(\mathbb{Z}^2) = (\mathbb{Z} + \sqrt{2}\mathbb{Z}) \cdot (1, \sqrt{2})$. D'après la question précédente, $(\mathbb{Z} + \sqrt{2}\mathbb{Z})$ est dense dans $\mathbb{R}$ et donc $\pi(\mathbb{Z}^2)$, dense dans V, n'est pas un réseau.

(3) C'est un exercice classique. Soit G un sous-groupe non trivial de $\mathbb{R}$. En particulier il est non-vide, et il existe donc au moins un élément strictement positif. Ceci nous permet de définir $\alpha = \inf G \cap \mathbb{R}_+^*$. Il y a alors deux cas de figure :

- **Cas $\alpha = 0$:** Dans ce cas G est dense. En effet, par la propriété de la borne inférieure et la définition de α, pour tout $\epsilon > 0$ on peut trouver $g \in G$ tel que $0 < g < \epsilon$. Soit $x \in \mathbb{R} \setminus G$ et notons $\lfloor a \rfloor$ le plus grand entier inférieur à un réel a, satisfaisant $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$. Comme G est un groupe additif, on a $\lfloor x/g \rfloor g \in G$. On a de plus $0 \leq x - \lfloor x/g \rfloor g = g(x/g - \lfloor x/g \rfloor) < \epsilon$, ce qu'on voulait démontrer.
- **Cas $\alpha > 0$:** On a directement que G est discret, puisque l'intervalle $(-\alpha/2, \alpha/2)$ ne contient que 0, donc par translation par les éléments de $g \in G$, les intervalles $(g - \alpha/2, g + \alpha/2)$ ne contiennent qu'un seul élément de G. Il faut montrer que $\alpha \in G$, puis que $G = \alpha\mathbb{Z}$. Deux utilisations de la propriété de la borne inférieure donnent $g, g' \in G$ tels que $\alpha \leq g < g' < 2\alpha$. Ceci entraine que $0 < g' - g \leq \alpha$, et donc par définition de α que $\alpha = g' - g \in G$. Il est ensuite clair que $\alpha\mathbb{Z} \subset G$. Pour l'autre inclusion, notons que pour tout $g \in G$, on a $g - \lfloor g/\alpha \rfloor \alpha \in G$. Par définition, ceci implique $0 \leq \alpha(g/\alpha - \lfloor g/\alpha \rfloor) < \alpha$, ce qui n'est possible que si $g = \lfloor g/\alpha \rfloor \alpha$.

3 (1) Si on a seulement une famille génératrice $\mathbf{G}$ (sous forme matricielle) pour $\mathcal{L}$, on commence par la mettre en forme normale de Hermite, mettons $\mathbf{H}$. D'après le cours, ceci est faisable en $O(mn^4)$. On montre que les r première colonnes non

nulles de $\mathbf{H}$ forment une base de $\mathcal{L}$. En effet, les propriétés de la HNF donnent l'existence d'une matrice $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ telle que $\mathbf{G} = [\mathbf{H}|\mathbf{0}] \cdot \mathbf{U}$. Autrement dit, il existe une sous-matrice $\mathbf{V} \in \mathbb{Z}^{r \times n}$ de $\mathbf{U}$ telle que $\mathbf{G} = \mathbf{HV}$, et encore autrement dit, on a $\mathcal{L} \subset \mathcal{L}(\mathbf{H})$. Comme $\mathbf{U}$ est unimodulaire, un argument symétrique montre que $\mathcal{L}(\mathbf{H}) \subset \mathcal{L}$. Enfin, on sait que le rang de $\mathbf{H}$ est la dimension de l'espace engendré par les colonnes de $\mathbf{G}$.

(2) D'après la question précédente, on peut supposer que $\mathcal{L}$ est donné par une base $\mathbf{B}$ sous forme matricielle. On note $\mathbf{B}^\dagger = \mathbf{B}^{-1}$ si $\mathbf{B}$ est carrée et $\mathbf{B}^\dagger = (\mathbf{B}^t\mathbf{B})^{-1}\mathbf{B}^t$ si $\mathbf{B}$ est rectangulaire (avec plus de lignes que de colonnes). L'algorithme calcule $\mathbf{z} = \mathbf{B}^\dagger\mathbf{v}$, et vérifie que $\mathbf{v} \in \mathbb{Z}^n$. L'opération la plus chère (hormis le calcul de $\mathbf{B}$) est l'inversion, qu'on peut faire en $O(n^3)$ opérations par exemple avec l'algorithme du pivot de Gauss.

(3) Il y a certainement plusieurs méthodes. Une approche simple consiste à calculer les HNF de systèmes générateurs de $\mathcal{L}$ et $\mathcal{L}'$ et de vérifier si elles sont égales. Si elles le sont, par unicité de la forme de Hermite, les deux réseaux sont égaux aussi. Sinon, on a obtenu deux matrices $\mathbf{B}, \mathbf{B}'$ représentant des bases de ces réseaux, et supposer sans perte de généralité que $\operatorname{rk}\mathbf{B} \geq \operatorname{rk}\mathbf{B}'$. On calcule alors la matrice $\mathbf{B}^\dagger$ (voir la question précédente) et on vérifie si $\mathbf{B}^\dagger\mathbf{B}'$ est une matrice entière. Dans ce cas, $\mathcal{L}' \subset \mathcal{L}$, sinon, il n'y a pas inclusion.

(4) Il est clair que la concaténation $\mathbf{M} = [\mathbf{G}|\mathbf{G}']$ des systèmes générateurs de $\mathcal{L}$ et $\mathcal{L}'$ est un système générateur de la somme. On en obtient une base à l'aide la HNF. Ceci donne une autre méthode pour tester l'inclusion entre deux réseaux. Supposons (sans perte de généralités) que $\mathcal{L}' \subset \mathcal{L}$. Alors $\mathcal{L} + \mathcal{L}' = \mathcal{L}$ et donc la forme de Hermite de $\mathbf{M}$ est une base de $\mathcal{L}$, qui doit donc être égale à la forme de Hermite de $\mathbf{G}$.

4 (1) Si $b_1, \ldots, b_n$ est une base de $\mathcal{L}$, c'est en particulier une base de V qui est donc de dimension $n = \operatorname{rk}\mathcal{L}$. Alors, la base duale $b_1^\vee, \ldots, b_n^\vee$ de V, définie par $\langle b_i^\vee, b_j\rangle = 1$ si et seulement si $i = j$ et 0 sinon, engendre au moins un sous-réseau de rang n de $\mathcal{L}^\vee$. Soit maintenant $x \in \mathcal{L}^\vee$, qu'on peut donc écrire $x = \sum_i x_i b_i^\vee$, avec les $x_i \in \mathbb{R}$ *a priori*. Pour tout $j \leq n$, on a $\langle x, b_j\rangle = x_i \in \mathbb{Z}$ par définition du dual : une base de $\mathcal{L}^\vee$ est la duale de la base de $\mathcal{L}$. Sous forme matricielle, si on appelle $\mathbf{D}$ la base duale de $\mathbf{B}$, on doit avoir $\mathbf{D}^t\mathbf{B} = I_n$. Si $\mathcal{L}$ est de rang m, on a $\mathbf{D} = \mathbf{B}^{-t}$, et sinon, on peut vérifier que $\mathbf{D} = \mathbf{B}(\mathbf{B}^t\mathbf{B})^{-1}$.

(2) Vu les expressions matricielles, ou même la résolution de la première question, l'égalité $\mathcal{L}^{\vee\vee} = \mathcal{L}$ est immédiate. La seconde identité est obtenue par double inclusion : si $v \in (\mathcal{L}_1 + \mathcal{L}_2)^\vee$, on a $\langle v, u_1 + u_2\rangle \in \mathbb{Z}$ pour tout $u_i \in \mathcal{L}_i$. En prenant en particulier $u_1 = 0$ ou $u_2 = 0$, on obtient $(\mathcal{L}_1 + \mathcal{L}_2)^\vee \subset \mathcal{L}_1^\vee \cap \mathcal{L}_2^\vee$. L'autre sens est encore plus simple. Pour la troisième identité, il suffit de comparer les duals de $(\mathcal{L}_1 \cap \mathcal{L}_2)^\vee$ et $\mathcal{L}_1^\vee + \mathcal{L}_2^\vee$ à l'aide des deux premières identités.

(3) D'après la question précédente, une base de $\mathcal{L}_1 \cap \mathcal{L}_2$ est la duale d'une base de $\mathcal{L}_1^\vee + \mathcal{L}_2^\vee$. Sous forme matricielle, calculer la duale d'une base coûte de l'ordre d'une inversion de matrice. D'après l'exercice précédent, on sait calculer des bases pour $\mathcal{L}_1, \mathcal{L}_2$ par forme de Hermite. On peut donc obtenir des bases pour $\mathcal{L}_1^\vee, \mathcal{L}_2^\vee$ au prix de deux inversions de matrices (moins chères que la HNF), puis on peut en déduire une base pour la somme par forme de Hermite encore une fois. C'est cette étape qui domine : la concaténation des bases est de dimension au plus $m \times 2m$, sans compter le déterminant. Une fois une base de $\mathcal{L}_1^\vee + \mathcal{L}_2^\vee$ obtenue, on obtient

sa duale par inversion de matrice. Le nombre d'opérations de l'étape la plus chère est au pire en $O(m^5)$.

5 (1) Soient $\mathbf{B}$ et $\mathbf{B}'$ deux bases (sous forme de matrices) de $\mathcal{L}$ et $\mathcal{L}'$ respectivement. Par hypothèse, il existe une matrice $\mathbf{U} \in \mathcal{M}_n(\mathbb{Z})$ telle que $\mathbf{B}' = \mathbf{B}\mathbf{U}$. Comme $\mathbf{B}'$ est de rang plein, on a $\det \mathbf{U} \neq 0$. D'autre part, $\mathbf{U}$ est entière et comme $\mathcal{L}' \neq \mathcal{L}$, on a nécessairement $|\det \mathbf{U}| > 1$. On conclut par définition du déterminant d'un réseau.

(a) Soit $\mathbf{x} \in \mathbb{R}^n$, et écrivons $\mathbf{x} = \sum_i x_i \mathbf{b}_i$, où les $\mathbf{b}_i$ sont les vecteurs colonnes de $\mathbf{B}$. En notant $\lceil \cdot \rfloor$ la partie entière d'un réel et $\{\cdot\}$ sa partie fractionnaire, on peut décomposer $\mathbf{x} = \sum_i \lceil x_i \rfloor \mathbf{b}_i + \sum_i \{x_i\} \mathbf{b}_i$, où le premier vecteur est dans $\mathcal{L}$ et le second dans $\mathcal{D}_{\mathbf{B}}$. Montrons maintenant que cette décomposition est unique. Supposons que $\mathbf{x} \in \mathbf{u} + \mathcal{D}_{\mathbf{B}} \cap \mathbf{u}' + \mathcal{D}_{\mathbf{B}}$, de sorte que $\mathbf{x} = \mathbf{y} + \mathbf{u} = \mathbf{y}' + \mathbf{u}'$ pour $\mathbf{y}, \mathbf{y}'$ dans $\mathcal{D}_{\mathbf{B}}$. Ceci implique que $\mathbf{y} - \mathbf{y}' \in \mathcal{L}$. Si $(y_i)_i$, $(y'_i)_i$ sont les coordonnées respectives de $\mathbf{y}, \mathbf{y}'$ dans la base $\mathbf{B}$, on remarque $\max_i |y_i - y'_i| < 1$, donc $\mathbf{y} = \mathbf{y}'$ et par extension $\mathbf{u} = \mathbf{u}'$.

(b) On se convainc par un dessin qu'il s'agit de montrer qu'il n'y a qu'une copie de $\mathcal{D}_{\mathbf{B}}$ dans $\mathcal{D}_{\mathbf{B}'}$ par classes de $\mathcal{L}/\mathcal{L}'$. Il s'agit ensuite d'utiliser les propriétés élémentaires du volume (ou plus généralement de la mesure de Lebèsgue) :

$$\begin{aligned}\sum_{\mathbf{x} \in \mathbf{u} + \mathcal{L}'} \mathrm{Vol}\big(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{x} + \mathcal{D}_{\mathbf{B}})\big) &= \sum_{\mathbf{u}' \in \mathcal{L}'} \mathrm{Vol}(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{x} + \mathbf{u} + \mathcal{D}_{\mathbf{B}})) \\ &= \sum_{\mathbf{u}' \in \mathcal{L}'} \mathrm{Vol}\big((\mathcal{D}_{\mathbf{B}'} - \mathbf{u}) \cap (\mathbf{x} + \mathcal{D}_{\mathbf{B}})\big) \\ &= \mathrm{Vol}(\mathbf{x} + \mathcal{D}_{\mathbf{B}}),\end{aligned}$$

où on utilise l'invariance du volume par translation à la deuxième ligne, et la question (1) à la troisième. On conclut encore par invariance par translation.

(c) D'après la question (1) on a $\mathcal{D}_{\mathbf{B}'} = \bigcup_{\mathbf{u} \in \mathcal{L}} (\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{u} + \mathcal{D}_{\mathbf{B}}))$. Un réseau étant dénombrable, on en déduit $\mathrm{Vol}(\mathcal{D}') = \sum_{\mathbf{u} \in \mathcal{L}} \mathrm{Vol}(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{u} + \mathcal{D}_{\mathbf{B}}))$. Les classes $\bar{\mathbf{u}}$ de $\mathcal{L}/\mathcal{L}'$ correspondent aux "cosets" $\mathbf{u} + \mathcal{L}'$, ce qui donne

$$\begin{aligned}\mathrm{Vol}(\mathcal{D}') &= \sum_{\bar{\mathbf{u}} \in \mathcal{L}/\mathcal{L}'} \sum_{\mathbf{x} \in \mathbf{u} + \mathcal{L}'} \mathrm{Vol}\big((\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{u} + \mathcal{D}_{\mathbf{B}})\big) \\ &= \sum_{\bar{\mathbf{u}} \in \mathcal{L}/\mathcal{L}'} \mathrm{Vol}(\mathcal{D}),\end{aligned}$$

d'après la question précédente. Comme $\mathrm{Vol}(\mathcal{D}')$ est fini, $\mathcal{L}/\mathcal{L}'$ est nécessairement un groupe fini et avec la définition du déterminant d'un réseau, on obtient le résultat.