Réseaux euclidiens et cryptographie

Journées Télécom-UPS
« Le numérique pour tous »

David A. Madore
Télécom ParisTech
david.madore@enst.fr

29 mai 2015

Plan

Réseaux euclidiens : définition

- Un **réseau** de $\mathbb{R}^m$ est un sous-groupe (additif) discret L de l'espace euclidien $\mathbb{R}^m$.

Un tel sous-groupe est nécessairement isomorphe à $\mathbb{Z}^n$ (où $n \leq m$) comme groupe abélien : il existe $b_1, \ldots, b_n \in L$ tels que $L = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n$.

De plus, $b_1, \ldots, b_n$ sont $\mathbb{R}$-libres (=linéairement indép$^{\text{ts}}$).

On dit qu'ils sont une **base** de L, et que n est le **rang** de L.

Définition équivalente :

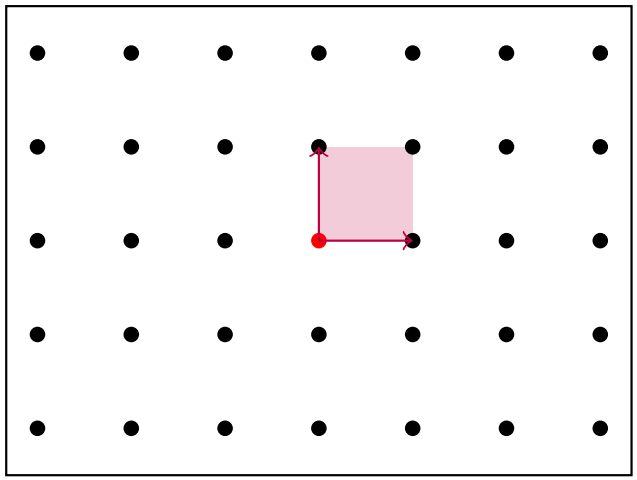
- Un **réseau** de $\mathbb{R}^m$ est un $\mathcal{L}(B) := \{uB : u \in \mathbb{Z}^n\}$ où $B \in \mathbb{R}^{n \times m}$ est une matrice de rang n.

(B est la matrice dont les b_i sont les lignes.)

- On suppose souvent $m = n$ (réseau de *rang plein*), quitte à se placer dans $\mathrm{Vect}_{\mathbb{R}}(L) = \mathbb{R}b_1 \oplus \cdots \oplus \mathbb{R}b_n$.

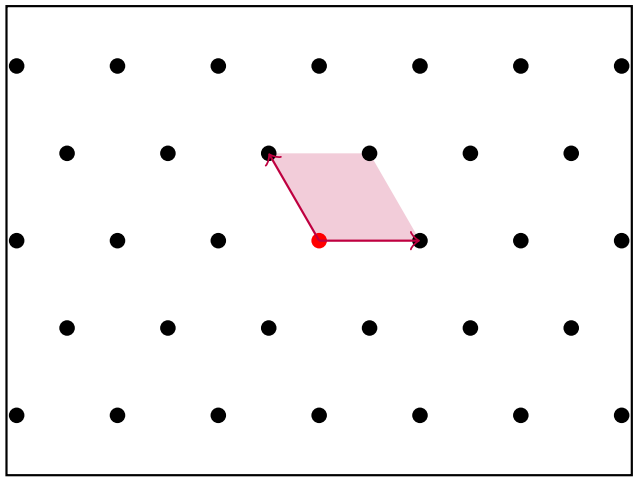
Exemples

Les deux réseaux de rang 2 admettant le plus grand groupe de symétries sont (à similitude près) :



$(A_1)^2$

$\mathbb{Z}^2 \subseteq \mathbb{R}^2$



A_2

$\{(x, y, z) \in \mathbb{Z}^3 : x + y + z = 0\} \subseteq \mathbb{R}^3$

Bases et parallélotopes fondamentaux

Soit $\mathcal{L}(B) = \{uB : u \in \mathbb{Z}^n\} \subseteq \mathbb{R}^m$ (où $\operatorname{rg} B = n$).

- $\mathcal{P}(B) := \{uB : u \in [0;1[^n\}$ s'appelle **parallélotope fondamental** associé à la base B.

- On a $\mathcal{L}(B) = \mathcal{L}(B')$ ssi $B' = UB$ où $U \in GL_n(\mathbb{Z})$.

Ici, $GL_n(\mathbb{Z})$ est l'ensemble des matrices $n \times n$ à coefficients entiers, de déterminant ± 1 (**unimodulaires**).

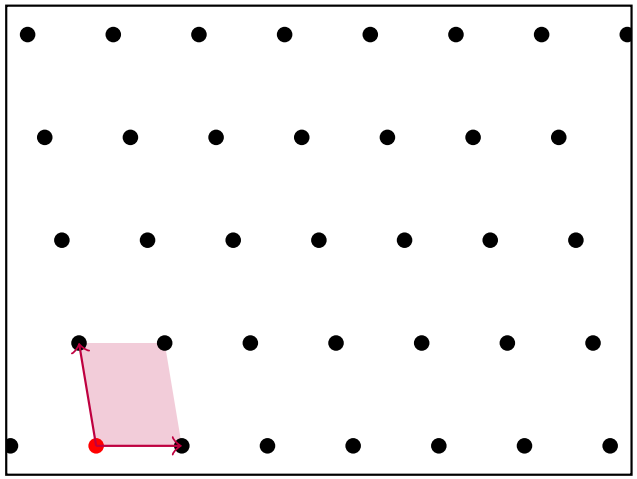
Dès que $n > 1$, un réseau admet une infinité de bases.

On peut voir l'ensemble des réseaux de rang plein dans $\mathbb{R}^n$ comme l'ensemble quotient $GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$.

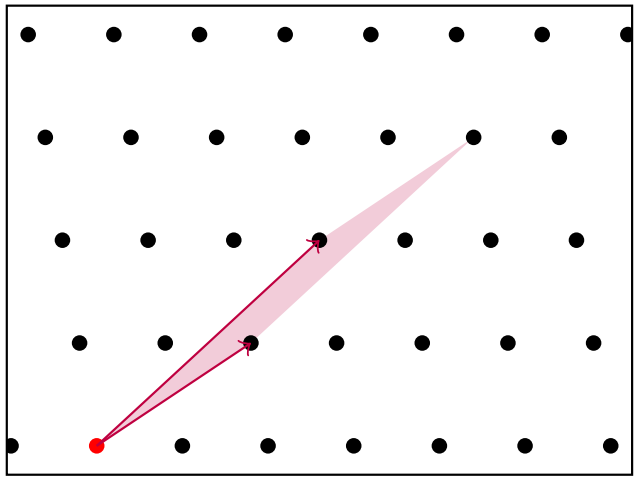
- $\operatorname{vol}(\mathcal{P}(B)) =: \operatorname{covol}(\mathcal{L}(B)) = |\det(B)|$ (lorsque $m = n$) : volume du parallélogramme fondamental : **(co)volume** ou **déterminant** du réseau. Ne dépend pas de B !

Toutes les bases ne se valent pas

Certaines bases sont plus « agréables » que d'autres :



« Bonne » base



Moins « bonne » base

Les deux parallélogrammes fondamentaux dessinés ont la même aire, mais pas la même forme / la même longueur des côtés.

« Bonne » $\approx$ constituée de petits vecteurs.

Thèmes : Comment construire de « bonnes » bases à partir de « mauvaises » ? (Par des opérations élémentaires entières sur les lignes de B.) Comment exploiter la difficulté de ce problème ?

Similitudes

Soit $\mathcal{L}(B) = \{uB : u \in \mathbb{Z}^n\} \subseteq \mathbb{R}^m$ (où $\operatorname{rg} B = n$).

- Si $t \in \mathbb{R}^\times$, on a $t \cdot \mathcal{L}(B) = \mathcal{L}(tB)$ (*homothétie*).

Multiplie le covolume par t^n.

- Si $\Omega \in O_m$, on a $\mathcal{L}(B) \cdot \Omega = \mathcal{L}(B\Omega)$ (*isométrie*).

Ne change pas le covolume.
Si $\mathcal{L}(B) \cdot \Omega = \mathcal{L}(B)$, on dit que Ω est une **symétrie** de $\mathcal{L}(B)$.

On identifie souvent deux réseaux homothétiques, isométriques, ou les deux (semblables).
Ceci permet de **normaliser** $\operatorname{covol}(L) = 1$.

On peut considérer $SL_n^{\pm}(\mathbb{R})/O_n$ comme l'espace des *formes de parallélotopes* de dimension n [espace riemannien symétrique], et $GL_n(\mathbb{Z})\backslash SL_n^{\pm}(\mathbb{R})/O_n$ comme l'espace des *formes de réseaux* de rang plein.

- **Matrice de Gram :** $G := BB^{\mathrm{tr}}$ soit $G_{ij} = b_i \cdot b_j$, invariante par isométrie ($B\Omega(B\Omega)^{\mathrm{tr}} = BB^{\mathrm{tr}}$).

Matrice de Gram

Soit $\mathcal{L}(B) = \{uB : u \in \mathbb{Z}^n\} \subseteq \mathbb{R}^m$ (où $\operatorname{rg} B = n$).

Matrice de Gram : $G := BB^{\mathrm{tr}}$ soit $G_{ij} = b_i \cdot b_j$.

- Invariante par isométrie ($B\Omega(B\Omega)^{\mathrm{tr}} = BB^{\mathrm{tr}}$ si $\Omega \in O_m$).
- Est la matrice de la forme quadratique sur $\mathbb{Z}^n$ définie par $q(u) = \|uB\|^2$ (norme euclidienne transportée au réseau), donc définie positive. ($\Rightarrow$ Lien avec les f.q. sur les entiers.)
- Vérifie $\det(G) = \operatorname{covol}(L)^2$ (**discriminant** de $L = \mathcal{L}(B)$).

En effet, $\det(G) = \det(B)^2$ est évident si $m = n$.

- Réciproquement, si G est définie positive, on peut écrire $G = BB^{\mathrm{tr}}$ pour $B \in GL_n(\mathbb{R})$ (conséquence de Cholesky ou du théorème spectral), et B est unique à isométrie près.

L'espace $SL_n^{\pm}(\mathbb{R})/O_n$ s'identifie donc à l'ensemble des matrices définies positives de déterminant 1, et $GL_n(\mathbb{Z})\backslash SL_n^{\pm}(\mathbb{R})/O_n$ à l'ensemble des formes quadratiques définies positives sur un $\mathbb{Z}$-module de rang n.

Orthogonalisation de Gram-Schmidt

- Si $b_1, \ldots, b_n \in \mathbb{R}^m$ sont $\mathbb{R}$-libres, on définit par récurrence $b_i^\star := b_i - \sum_{j<i} \mu_{i,j}\, b_j^\star$ où $\mu_{i,j} := (b_i \cdot b_j^\star)/\|b_j^\star\|^2$ (i.e., $b_i^\star = \mathrm{proj}_{\mathrm{Vect}(b_j : j<i)^\perp}(b_i)$).

Les $(b_i^\star)_{i \le s}$ sont donc une base orthogonale de $\mathrm{Vect}(b_i^\star : i \le s) = \mathrm{Vect}(b_i : i \le s)$.

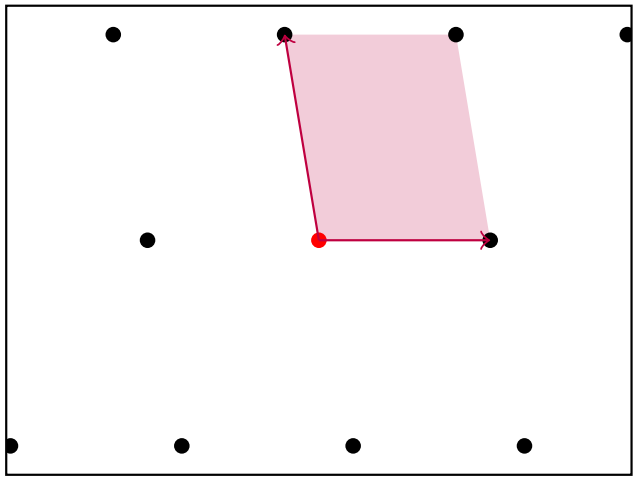
- Formulation matricielle (pour $m = n$) : $B = MDV$ avec M triangulaire inférieure de diagonale 1 (soit : $M_{ij} = \mu_{i,j}$ si $j < i$, 1 si $j = i$, et 0 si $j > i$), D diagonale de diagonale $\|b_i^\star\|$, et V orthogonale.

En particulier, $|\det(B)| = \det D = \prod_{i=1}^n \|b_i^\star\|$.

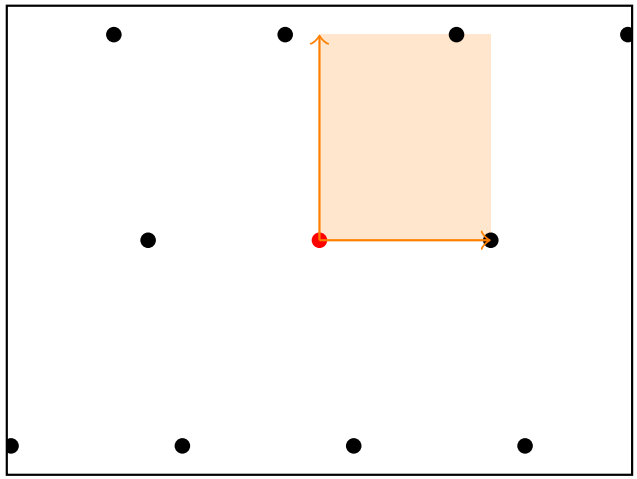
- Dépend de l'ordre : si on permute $b_i \leftrightarrow b_{i+1}$, alors $(b_i^\star, b_{i+1}^\star)$ devient $(b_{i+1}^\star + \mu_{i+1,i}\, b_i^\star,\ \frac{\|b_{i+1}^\star\|^2\, b_i^\star - \mu_{i+1,i}\, \|b_i^\star\|^2\, b_{i+1}^\star}{\|b_{i+1}^\star\|^2 + \mu_{i+1,i}^2\, \|b_i^\star\|^2})$.

Gram-Schmidt (suite)

Calcul de l'aire d'un parallélogramme :



(b_1, b_2)



$(b_1^\star, b_2^\star)$

La matrice (DV) des $b_i^\star$ définit un parallélotope rectangle ayant le même volume $\mathrm{covol}(L)$ que celui défini par les b_i.

Les $b_i^\star$ n'appartiennent pas à L en général.

Minima successifs d'un réseau

Soit L un réseau euclidien de rang n dans $\mathbb{R}^m$. On définit, pour $1 \leq i \leq n$:

$$\lambda_i(L) = \min\{r \in \mathbb{R}_+ : \dim \mathrm{Vect}(L \cap \mathrm{B_f}(0,r)) \geq i\}$$

où $\mathrm{B_f}(0,r) = \{x \in \mathbb{R}^m : \|x\| \leq r\}$.

Autrement dit, $\lambda_i(L)$ est le plus petit r tel qu'on puisse trouver i vecteurs $\mathbb{R}$-libres tous de norme $\leq r$ dans L.

Attention : $L \cap \mathrm{B_f}(0,\lambda_n)$ ne contient pas forcément une $\mathbb{Z}$-base de L.

En particulier, $\lambda_1(L) = \min\{\|x\| : x \in L \setminus \{0\}\}$ est la norme du plus petit vecteur non nul de L.

Exercice : Montrer que $\lambda_1(L) \geq \min\{\|b_i^\star\| : 1 \leq i \leq n\}$.
Indication : $\|uMDV\| = \|uMD\|$ avec MDV comme dans G-S.

Question : Peut-on borner $\lambda_1(L)\ \mathrm{covol}(L)^{-1/n}$?

Empilements de sphères

Ici, L est de rang plein.

Soit $\rho(L) := \frac{1}{2}\lambda_1(L)$. Il s'agit du plus grand rayon ρ tel que les boules ouvertes de rayon ρ centrées sur les points de L soient deux à deux disjointes.

La **densité** = fraction du volume occupé par les boules vaut alors $\mathscr{V}_n\ \rho(L)^n / \operatorname{covol}(L)$ où[†] $\mathscr{V}_n := \frac{\pi^{n/2}}{(n/2)!}$ est le volume de la n-boule unité.

Il est souvent plus commode de travailler avec $\rho(L)^n / \operatorname{covol}(L)$, ou encore $\lambda_1(L)\ \operatorname{covol}(L)^{-1/n}$.

Question : Quelles valeurs ces nombres peuvent-ils prendre ? (Quel réseau empile le mieux les boules en dimension n ?) Réponse connue pour $n \leq 8$ et $n = 24$.

Constante de Hermite :
$\gamma_n := \sup\{\lambda_1(L)^2 : L \text{ t.q. } \operatorname{covol}(L) = 1\}$ (atteint ; on a alors $\gamma_1 = 1$, $\gamma_2 = \frac{2}{3}\sqrt{3}$, $\gamma_3 = \sqrt[3]{2}$, $\gamma_8 = 2$, $\gamma_{24} = 4$).

[†]Où $(k+\frac{1}{2})! := \frac{(2k+1)!!}{2^{k+1}}\sqrt{\pi}$ (et $(2k+1)!! = \prod \text{impairs}$).

Une borne de Minkowski

Explicitons le fait que la densité d'un empilement est ≤ 1.

Théorème (Blichfeld) : Si $L \subseteq \mathbb{R}^n$ de rg. pl., et $S \subseteq \mathbb{R}^n$ t.q. $\mathrm{vol}(S) > \mathrm{covol}(L)$, alors $\exists z_1 \neq z_2 \in S$ t.q. $z_1 - z_2 \in L$.

Preuve : sinon, les $S_z := (S + z) \cap \mathcal{P}$ sont disjoints (pour $z \in L$). Or $\sum_z \mathrm{vol}(S_z) = \sum \mathrm{vol}(S_z - z) = \mathrm{vol}\, S > \mathrm{vol}\, \mathcal{P}$, contradiction.

Théorème (Minkowski) : Si $L \subseteq \mathbb{R}^n$ de rg. pl., et S convexe sym$^{\text{que}}$ t.q. $\mathrm{vol}(S) > 2^n \,\mathrm{covol}(L)$, alors $S \cap (L \setminus \{0\}) \neq \varnothing$.

Preuve : $\mathrm{vol}(\frac{1}{2}S) = 2^{-n}\,\mathrm{vol}(S) > \mathrm{covol}(L)$ donc il existe $z_1 \neq z_2 \in \frac{1}{2}S$ t.q., $z_1 - z_2 \in L$, or $z_1 - z_2 = \frac{1}{2}(2z_1 - 2z_2) \in S$.

Corollaire : $\lambda_1(L) \leq \sqrt{n}\,\mathrm{covol}(L)^{1/n}$ (c'est-à-dire, $\gamma_n \leq n$).

Preuve : Appliquer le théorème à la boule ouverte de centre 0 et rayon λ_1, et utiliser la minoration $\mathscr{V}_n \geq (2/\sqrt{n})^n$ (car la boule unité contient un cube de côté $2/\sqrt{n}$).

Amélioration : $(\prod_{i=1}^n \lambda_i(L))^{1/n} \leq \sqrt{n}\,\mathrm{covol}(L)^{1/n}$.

Idée : Remplacer la boule par l'ellipsoïde de demi-axes $\lambda_1, \ldots, \lambda_n$ orientés selon le Gram-Schmidt des minima successifs.

Le réseau dual

Si $L \subseteq \mathbb{R}^n$ est un réseau de rang plein, son **dual** est

$$L^* := \{y \in \mathbb{R}^n : \forall x \in L,\, x \cdot y \in \mathbb{Z}\}$$

où $x \cdot y$ est le produit scalaire (euclidien).

Matriciellement, si les vecteurs sont vus comme des vecteurs-lignes :

$$\begin{aligned} L^* &= \{y \in \mathbb{R}^n : \forall x \in L,\, xy^{\mathrm{tr}} \in \mathbb{Z}\} \\ &= \{y \in \mathbb{R}^n : \forall u \in \mathbb{Z}^n,\, uBy^{\mathrm{tr}} \in \mathbb{Z}\} \\ &= \{y \in \mathbb{R}^n : yB^{\mathrm{tr}} \in \mathbb{Z}^n\} = \mathcal{L}(B^{-\mathrm{tr}}) \end{aligned}$$

C'est donc aussi un réseau, et $(L^*)^* = L$. Covolume : $\mathrm{covol}(L^*) = \mathrm{covol}(L)^{-1}$. Homothéties : $(t \cdot L)^* = \frac{1}{t} \cdot L^*$.

Inverse la matrice de Gram. Cas de rang non plein : on peut définir $\mathcal{L}(B)^* = \mathcal{L}((G^{-1}B)^{\mathrm{tr}}) \subseteq \mathrm{Vect}_{\mathbb{R}}(\mathcal{L}(B))$.

Symétrie sur l'espace riemannien symétrique $SL_n^{\pm}(\mathbb{R})/O_n$.

Réseaux entiers

- Si $L \subseteq L^*$, i.e., si la matrice de Gram G est à coefficients entiers, on dit que L est **entier**.

Notamment, dans ce cas, le discriminant $\det G = \mathrm{covol}(L)^2$ est entier.

$\Rightarrow$ Lien avec les formes quadratiques entières ($q(u) = \|uB\|^2 = uGu^{\mathrm{tr}}$).

- On a $L = L^*$ ssi L est entier et $\mathrm{covol}(L) = 1$ (i.e., $G \in GL_n(\mathbb{Z})$). On dit alors que L est **unimodulaire**.

Si de plus $\|x\|^2 \in 2\mathbb{Z}$ pour tout $x \in L$ (i.e., q prend des valeurs paires), on dit que L est **pair** (=de type II), sinon **impair** (=de type I).

Le plus petit rang d'un réseau unimodulaire pair est 8, et ce réseau est unique à isométrie près (c'est E_8).

Quelques réseaux remarquables

- $\mathbb{Z}^n$ réseau entier de covolume 1, avec $\lambda_1 = \cdots = \lambda_n = 1$.
- $A_n := \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} : \sum_{i=0}^{n} x_i = 0\}$ réseau entier de covolume $\sqrt{n+1}$, avec $\lambda_1 = \cdots = \lambda_n = \sqrt{2}$.

Note : A_1 est isométrique à $\sqrt{2}\mathbb{Z}$, et A_2 est le réseau hexagonal, A_3 le « cubique faces centrées ».

- $A_n^* = A_n + \mathbb{Z}(-\frac{n}{n+1}, \frac{1}{n+1}, \frac{1}{n+1}, \ldots, \frac{1}{n+1})$ ici $\lambda_1 = \sqrt{\frac{n}{n+1}}$.

Note : A_1^* est isométrique à $\frac{1}{\sqrt{2}}\mathbb{Z}$ et A_2^* à $\frac{1}{\sqrt{3}}A_2$, et A_3^* est le « cubique centré ».

- $D_n := \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \in 2\mathbb{Z}\}$ réseau entier de covolume 2, avec $\lambda_1 = \cdots = \lambda_n = \sqrt{2}$.

Note : D_2 est isométrique à $\sqrt{2}\mathbb{Z}^2$, et D_3 est isométrique à A_3.

- $D_n^* = \mathbb{Z}^n \cup (\mathbb{Z} + \frac{1}{2})^n$, avec $\lambda_1 = 1$ si $n \geq 4$.

Note : D_4^* est isométrique à $\frac{1}{\sqrt{2}}D_4$.

- $E_8 := \{(x_1, \ldots, x_8) \in (\mathbb{Z}^8 \cup (\mathbb{Z} + \frac{1}{2})^8) : \sum_{i=1}^{8} x_i \in 2\mathbb{Z}\}$ réseau entier de covolume 1, avec $\lambda_1 = \cdots = \lambda_8 = \sqrt{2}$.

Quelques problèmes algorithmiques

Algorithmiquement, on considère généralement des réseaux $L \subseteq \mathbb{Z}^n$ (ou en tout cas $L \subseteq \mathbb{Q}^n$). Parfois $N\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$ (« N-modulaires »).

- **Problème $\mathbf{SVP}_h$** (« Shortest Vector Problem ») : pour $h \geq 1$, donnée une base B de $L = \mathcal{L}(B)$, trouver $z \in L$ tel que $0 \neq \|z\| \leq h \cdot \lambda_1(L)$.

SVP_h est NP-dur pour $h \lesssim \sqrt{n}$, polynomial (P) par LLL pour $h = 2^{n/2}$. $\mathrm{SVP} = \mathrm{SVP}_1$ est résoluble en complexité $2^{O(n)}$.

- **Problème $\mathbf{CVP}_h$** (« Closest Vector Problem ») : pour $h \geq 1$, donnée une base B de $L = \mathcal{L}(B)$ et $t \in \mathbb{R}^n$, trouver $z \in L$ tel que $\|t - z\| \leq h \cdot \mathrm{dist}(t, L)$.

CVP_h est au moins aussi dur que SVP_h, et polynomial (P) pour $h = 2^{n/2}$ par LLL+Babai.

Bases LLL-réduites

Gram-Schmidt : $b_i^\star := b_i - \sum_{j<i} \mu_{i,j}\, b_j^\star$ où $\mu_{i,j} := (b_i \cdot b_j^\star)/\|b_j^\star\|^2$.

La base $b_1, \ldots, b_n$ est dite LLL-δ-réduite ($\frac{1}{4} < \delta < 1$) si :

- pour tous $i > j$, on a $|\mu_{i,j}| \leq \frac{1}{2}$, et
- pour tout $i < n$, on a $\|b_{i+1}^\star + \mu_{i+1,i}\, b_i^\star\|^2 \geq \delta \cdot \|b_i^\star\|^2$.

Intuitivement, la première condition assure que les b_i ne sont pas trop loin d'être orthogonaux, et la seconde, qu'on ne gagne pas trop à échanger $b_i \leftrightarrow b_{i+1}$ avant d'appliquer G-S.

Notion de « bonne » base : on va voir que tout réseau a une base LLL-réduite, calculable en temps polynomial.

On déduit $\|b_{i+1}^\star\|^2 \geq (\delta - \mu_{i+1,i}^2)\|b_i^\star\|^2 \geq (\delta - \frac{1}{4})\|b_i^\star\|^2$.
Donc $\|b_i^\star\| \geq (\delta - \frac{1}{4})^{(i-1)/2}\|b_1\|$.
Comme $\lambda_1 \geq \min \|b_i^\star\|$, on a $\|b_1\| \leq (\delta - \frac{1}{4})^{-(n-1)/2}\lambda_1$.

Opérations élémentaires

- **Réduction** de la ligne b_i par b_j $(j < i)$: remplacer b_i par $b_i - cb_j$ (soit $B \leftarrow (1_n - cE_{ij})B$) où $c = \lceil \mu_{i,j} \rfloor$ (arrondi†).

Effet sur G-S : $\mu_{i,k} \leftarrow \mu_{i,k} - c\mu_{j,k}$, donc $\mu_{i,j} \leftarrow |\cdot| \leq \frac{1}{2}$.
Les $b_i^\star$ ne changent pas.

- **Réduction de taille** de la base :

pour i allant de 2 à n,
  pour j allant de $i-1$ à 1 (décroissant),
    réduire b_i par b_j (soit $b_i \leftarrow b_i - \lceil \mu_{i,j} \rfloor\, b_j$).

Assure la propriété $|\mu_{i,j}| \leq \frac{1}{2}$.

- **Échange** $b_i \leftrightarrow b_{i+1}$ [et recalculer / m.à.j. G-S !]

L'échange servira à assurer la propriété de Lovász
$\|b_{i+1}^\star + \mu_{i+1,i}\, b_i^\star\|^2 \geq \delta \cdot \|b_i^\star\|^2$.
Il faut refaire une réduction de taille après chaque échange !

†Soit $\lceil \xi \rfloor := \lfloor (\xi + \frac{1}{2}) \rfloor$ où $\lfloor \cdot \rfloor$ = partie entière.

L'algorithme LLL

Soit $\frac{1}{4} < \delta < 1$ (typiquement $\delta = \frac{3}{4}$ ou mieux $\frac{1}{4} + (\frac{3}{4})^{n/(n-1)}$).

Algorithme de Lenstra-Lenstra-Lovász donnés $b_1, \ldots, b_n$ base d'un réseau L de $\mathbb{R}^m$, calcule une base LLL-δ-réduite.

- (1) Calculer (ou m.à.j.) Gram-Schmidt.
- (2) Réduction de taille de la base :

pour i allant de 2 à n,
  pour j allant de $i-1$ à 1 (décroissant),
    réduire b_i par b_j (soit $b_i \leftarrow b_i - \lceil \mu_{i,j} \rfloor \, b_j$)
      (et $\mu_{i,k} \leftarrow \mu_{i,k} - \lceil \mu_{i,j} \rfloor \, \mu_{j,k}$).

- (3) S'il existe i tel que $\|b_{i+1}^\star + \mu_{i+1,i} \, b_i^\star\|^2 < \delta \cdot \|b_i^\star\|^2$:
  échanger $b_i \leftrightarrow b_{i+1}$, et retourner en (1).

Théorème : LLL termine en temps polynomial.

Idée : $\prod_{i=1}^n \|b_i^\star\|^{2(n-i+1)} = \prod_{i=1}^n \mathrm{covol}(\mathcal{L}(b_1, \ldots, b_i))^2$ décroît d'un facteur δ pour chaque échange.

Note : pour $n = 2$, LLL $\cong$ algo. de Lagrange|Gauß $\approx$ « Euclide centré ».

Propriétés des bases LLL-réduites

Soit $\alpha = \frac{1}{\delta - \frac{1}{4}}$ et $b_1, \ldots, b_n$ une base LLL-δ-réduite.

On a vu $\|b_1\| \leq \alpha^{(n-1)/2}\, \lambda_1$, donc pour $\delta = \frac{3}{4}$ on a $\|b_1\| \leq 2^{(n-1)/2}\, \lambda_1$ et LLL résout SVP$|_h$ pour $h = 2^{(n-1)/2}$ (renvoyer b_1) en temps poly.

Plus généralement, on a :

- $\|b_i\| \leq \alpha^{(n-1)/2}\, \lambda_i$
- $\|b_1\| \leq \alpha^{(n-1)/4}\, \mathrm{covol}(L)^{1/n}$
- $\prod_{i=1}^{n} \|b_i\| \leq \alpha^{n(n-1)/4}\, \mathrm{covol}(L)$

Expérimentalement, sur des réseaux et bases aléatoires, on observe des inégalités meilleures (mais toujours exponentielles), par exemple $\|b_1\| \leq 1.022^n\, \mathrm{covol}(L)^{1/n}$.

Algorithme de Babai

Soit $L = \mathcal{L}(B)$ un réseau et $t \in \mathbb{R}^n$. On veut résoudre le problème CVP_h avec $h = 2^{n/2}$, i.e., trouver $z \in L$ tel que $\|z - t\| \leq 2^{n/2} \operatorname{dist}(t, L)$.

- Appliquer LLL avec $\delta = \frac{3}{4}$ à B.
- Faire $x \leftarrow t$, puis
  pour j allant de n à 1 (décroissant),
  remplacer $x \leftarrow x - cb_j$
  où $c = \lceil (b \cdot b_j^\star)/\|b_j^\star\|^2 \rfloor$.
- Retourner $z = t - x$.

De façon équivalente : on choisit d'abord $c \in \mathbb{Z}$ tel que l'hyperplan affine $cb_n^\star + \text{Vect}(b_1, \ldots, b_{n-1})$ soit aussi proche que possible de t, puis on applique récursivement pour trouver un élément proche de x dans $cb_n + \mathcal{L}(b_1, \ldots, b_{n-1})$ (i.e., proche de $x - cb_n$ dans $\mathcal{L}(b_1, \ldots, b_{n-1})$).

Approximation diophantienne simultanée

- Soient $(\xi_1, \ldots, \xi_r) \in \mathbb{R}$ irrationnels. On cherche à approcher les ξ_i par des rationnels p_i/q *de même dénominateur*, i.e., trouver $(p_1, \ldots, p_r) \in \mathbb{Z}^r$ et $q \in \mathbb{N}_{>0}$ tels que les $|q\xi_i - p_i|$ soient petits et q pas trop grand. Qualité prédite par :
- **Dirichlet :** Il existe des q arbitrairement grands tels que $|q\xi_i - p_i| \leq q^{-1/r}$ où $p_i = \lceil q\xi_i \rfloor$.

Preuve : Découper $(\mathbb{R}/\mathbb{Z})^r$ en N^r cubes de côté $1/N$, et considérer les $N^r + 1$ classes des points $q\vec{\xi}$ pour $0 \leq q \leq N^r$: il existe $0 \leq q_1 < q_2 \leq N^r$ tels que les classes tombent dans la même boîte, et si $q = q_2 - q_1$ alors on a $|q\xi_i - p_i| \leq \frac{1}{N} \leq q^{-1/r}$.

- **Réseau :** pour $N > 0$ réel, considérer l'image de $\mathbb{Z}^{r+1} \to \mathbb{R}^{r+1}$ envoyant $(p_1, \ldots, p_r, q)$ sur $(N(q\xi_1 - p_1), \ldots, N(q\xi_r - p_r), q/N^r)$. On vient de voir que ce réseau a des petits vecteurs non nuls.
- LLL donne $|q\xi_i - p_i| \leq 2^{r/2}/N$ avec $q \leq 2^{r/2}N^r$.

Le problème du sac à dos

Problème : Donnés $a_1, \ldots, a_r, s$ entiers > 0, on cherche un sous-ensemble P de $\{1, \ldots, r\}$ tel que $\sum_{i \in P} a_i = s$ (supposé exister).

Approche par LLL : soit B une constante bien choisie ($\lceil \sqrt{n 2^n} \rceil$). considérer l'image de $\mathbb{Z}^{r+1} \to \mathbb{R}^{r+1}$ envoyant $(u_1, \ldots, u_r, v)$ sur $(u_1, \ldots, u_r, B \cdot (vs - \sum u_i a_i))$.

Avec les bonnes conditions sur les a_i (uniformément choisis sur un intervalle assez grand) et s (supérieur à $\frac{1}{2} \sum a_i$, ce qu'on peut toujours supposer), on montre qu'avec une probabilité extrêmement élevée, le plus court vecteur trouvé par LLL résout le problème du sac à dos.

Réseaux en cryptographie : principes

Utilisation pour le chiffrement à clé publique :

- La clé secrète sera typiquement une « bonne » base d'un réseau L (ou de son dual).

- La clé publique sera typiquement une « mauvaise » base du même réseau L.

Il est facile de générer la mauvaise base à partir de la bonne, difficile de faire l'opération inverse.

- Le chiffrement consiste à fabriquer un problème difficile à partir d'une mauvaise base, que la connaissance d'une bonne base permet de résoudre.

Par exemple : pour chiffrer, écrire le message sous forme d'un petit vecteur e, choisir z aléatoirement dans L, et renvoyer $x = z + e$. Déchiffrer demande de retrouver $z \in L$ proche de x.

Réseaux en cryptographie : espoirs et limitations

Espoirs de la cryptographie basée sur les réseaux :

- Résistance aux ordinateurs quantiques.

Contrairement aux problèmes de théorie des nombres (factorisation, pb. du log discret) utilisés comme source de difficulté en cryptographie à clé publique traditionnelle, et qui sont cassés par les ordinateurs quantiques[†], les problèmes de réseaux *paraissent* aussi difficiles pour les ordinateurs quantiques que pour les ordinateurs classiques.

- Outils plus puissants, p.ex., chiffrement complètement homomorphe ($\Rightarrow$calculs sur les chiffrés).

Limitations :

- Taille de clés/chiffrés beaucoup plus grande.
- Encore mal compris : pas de paramètres de sécurité standardisés.

[†]Si un jour ils existent vraiment...

Réseaux N-modulaires

Notation : $\mathbb{Z}_{/N} := \mathbb{Z}/N\mathbb{Z}$

Un réseau L tel que $N\mathbb{Z}^m \subseteq L \subseteq \mathbb{Z}^m$ est dit N-**modulaire**.
Équivalent à la donnée d'un sous-groupe $L/N\mathbb{Z}^m \subseteq \mathbb{Z}_{/N}^m$
(si $N{=}q$ premier, d'un sous-$\mathbb{F}_q$-esp. vect. de $\mathbb{F}_q^m$).

Attention : Le rang du réseau ici est m, même si $L/N\mathbb{Z}^m$ est très petit.

Si $A \in (\mathbb{Z}_{/N})^{n\times m}$ (typiquement, $n \leq m \approx n\log n$), soient :

$$\Lambda(A) := \mathcal{L}(A) + N\mathbb{Z}^m = \{x \in \mathbb{Z}^m : \exists u \in \mathbb{Z}^n,\, x \equiv uA\ [N]\}$$
$$\Lambda^\perp(A) := \{v \in \mathbb{Z}^m : Av^{\mathrm{tr}} \equiv 0\ [N]\}$$

les réseaux N-modulaires (de rang m) engendré par les lignes de A, resp. orthogonal aux lignes de A.

- On a $\Lambda^\perp(A) = N \cdot \Lambda(A)^*$ et $\Lambda(A) = N \cdot \Lambda^\perp(A)^*$.
- Si $N{=}q$ premier, et A de rang n, on a $\Lambda^\perp(A) = \Lambda(B)$ où $B \in \mathbb{Z}_{/q}^{(m-n)\times m}$ de rang $m-n$ (lignes de B base du suppl. ortho. des lignes de A, soit $BA^{\mathrm{tr}} = 0$).
- Avec haute probabilité, $\mathrm{covol}(\Lambda(A)) = q^{m-n}$ et $\mathrm{covol}(\Lambda^\perp(A)) = q^n$.

« Learning With Errors » (LWE)

Soit q premier. Typiquement, $10^3 < q < 10^5$ ici, $10^2 < n < 10^3$ et $10^3 < m < 10^4$.

Soit $A \in \mathbb{Z}_{/q}^{n \times m}$ tiré au hasard uniformément. Le vecteur $x \in \mathbb{Z}_{/q}^{m}$ est défini par l'un des deux procédés suivants :

- tiré au hasard uniformément dans $\mathbb{Z}_{/q}^{m}$, ou bien
- calculé par $x = uA + e$ où $u \in \mathbb{Z}_{/q}^{n}$ est tiré au hasard uniformément, et $e \in \mathbb{Z}_{/q}^{m}$ selon une distribution gaussienne (arrondie aux entiers et réduite mod q).

Défi : distinguer ces deux cas avec probabilité $> \frac{1}{2} + \varepsilon$.

Si l'écart-type est assez petit, application du CVP à x pour le réseau $\Lambda(A)$. Correction de l'« erreur » e.

Théorème (informel[t]) : pour un écart-type assez élevé dans la gaussienne ($> \sqrt{\frac{2\pi}{n}}$), LWE est au moins aussi difficile que certains problèmes difficiles « standards » sur les réseaux.

Un chiffrement basé sur LWE (Regev / GPV)

- Paramètre : $A \in \mathbb{Z}_{/q}^{n \times m}$ tiré au hasard uniformément. Clé secrète : $s \in \mathbb{Z}_{/q}^{m}$ selon une distribution gaussienne (« petit vecteur » secret). Clé publique : $p := As^{\mathrm{tr}} \in \mathbb{Z}_{/q}^{n}$.
- Chiffrement d'un bit $b \in \{0, 1\}$: tirer $u \in \mathbb{Z}_{/q}^{n}$ uniformément et $(e, e_0) \in \mathbb{Z}_{/q}^{m+1}$ selon une distribution gaussienne (« erreur »). Renvoyer $x = uA + e \in \mathbb{Z}_{/q}^{m}$ ainsi que $c = b\lfloor \frac{q}{2} \rfloor + u \cdot p + e_0 \in \mathbb{Z}_{/q}$.
- Déchiffrement : recevant $x \in \mathbb{Z}_{/q}^{m}$ et $c \in \mathbb{Z}_{/q}$, calculer $c - x \cdot s^{\mathrm{tr}}$, qui vaut $b\lfloor \frac{q}{2} \rfloor + e_0 - e \cdot s^{\mathrm{tr}}$: si ce nombre est plus proche de $\frac{q}{2}$, décoder 1, sinon, décoder 0. Validité : $e_0 - e \cdot s^{\mathrm{tr}}$ a une probabilité négligeable d'être $\gtrsim \frac{q}{2}$.

Le paramétrage de m, n, q et les écarts-types des gaussiennes doit être fait pour rendre le chiffrement difficile à casser et la probabilité d'erreur au décodage négligeable.

Un chiffrement basé sur LWE : explications

- Paramètre : $A \in \mathbb{Z}_{/q}^{n\times m}$. Clé secrète : $s \in \mathbb{Z}_{/q}^{m}$ (« petit vecteur »). Clé publique : $p := As^{\mathrm{tr}} \in \mathbb{Z}_{/q}^{n}$.

La clé publique est plutôt $(A|p) \in \mathbb{Z}_{/q}^{n\times(m+1)}$. Soit $L := \Lambda(A|p)$ le réseau engendré par ses lignes.

- Chiffrement : $x = uA + e \in \mathbb{Z}_{/q}^{m}$ et $c = b\lfloor\frac{q}{2}\rfloor + u \cdot p + e_0 \in \mathbb{Z}_{/q}$ où $u \in \mathbb{Z}_{/q}^{n}$ uniforme et $(e, e_0) \in \mathbb{Z}_{/q}^{m+1}$ « erreur ».

On a donc $(x|p) = u(A|p) + (e|e_0) + (0|b\lfloor\frac{q}{2}\rfloor) \in \mathbb{Z}_{/q}^{m+1}$ qui est soit proche de L, soit de $L + (0|\lfloor\frac{q}{2}\rfloor)$.

- La distinction entre ces deux cas est rendue possible par la connaissance du petit vecteur $(-s|1) \in \Lambda^{\perp}(A|p)$ (car on a $(A|p)(-s|1)^{\mathrm{tr}} = -As^{\mathrm{tr}} + p = 0$).

Moralité : Connaître un petit vecteur dans le réseau dual L^* permet de séparer nettement L en hyperplans.

Preuve de sécurité (idée)

Preuve en deux points :

- Savoir distinguer une clé publique $p \in \mathbb{Z}_{/q}^n$ (avec $p = As^{\mathrm{tr}}$ où $s \in \mathbb{Z}_{/q}^m$ petit vecteur) d'une clé aléatoire uniforme $\in \mathbb{Z}_{/q}^{n\times(m+1)}$ revient à savoir résoudre LWE.

En effet, se donner $p = As^{\mathrm{tr}}$ revient à se donner s modulo $\Lambda^\perp(A)$, c'est-à-dire un tirage $vB + s$ avec v uniforme, où $B \in \mathbb{Z}_{/q}^{(m-n)\times n}$ définit $\Lambda(B) = \Lambda^\perp(A)$. C'est bien un problème LWE.

- Savoir déchiffrer pour une clé $A' \in \mathbb{Z}_{/q}^{n\times(m+1)}$ aléatoire uniforme revient à savoir résoudre LWE.

En effet, il s'agit de distinguer $uA' + e'$ (avec u uniforme).