RÉSEAUX ET CRYPTOGRAPHIE

MASTER CSI, UE CRYPTANALYSE

CHRISTINE BACHOC

1. INTRODUCTION

Nous allons présenter quelques applications des réseaux euclidiens à la cryptographie, notamment l'utilisation de l'algorithme LLL dans quelques attaques classiques des cryptosystèmes.

2. RÉSEAUX EUCLIDIENS, DÉFINITIONS

L'espace euclidien $\mathbb{R}^n$ est muni de son produit scalaire usuel $x \cdot y = x_1y_1 + \cdots + x_ny_n$. Si $x \in \mathbb{R}^n$, on appelle norme de x la valeur de $x \cdot x$.

Définition 1. *Un réseau L de $\mathbb{R}^n$ est l'ensemble des combinaisons linéaires à coefficients entiers d'une base de $\mathbb{R}^n$*

$$L = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2 \oplus \cdots \oplus \mathbb{Z}b_n.$$

Exemples:

(1) Le réseau $L = \mathbb{Z}^n$ est appelé "réseau carré". Il a pour base la base canonique de $\mathbb{R}^n$.
(2) Le réseau hexagonal de dimension 2 a pour base les vecteurs de coordonnées $(1, 0)$ et $(1/2, \sqrt{3}/2)$. On le notera A_2.

Un réseau L admet plusieurs bases. Une famille de vecteurs $(e_1, \ldots, e_n)$ est une autre base de L si la matrice de passage de $(e_1, \ldots, e_n)$ à $(b_1, \ldots, b_n)$ est à coefficients entiers et a pour déterminant ± 1, c'est-à-dire si elle est inversible dans $M_n(\mathbb{Z})$. On note $Gl_n(\mathbb{Z})$ le groupe des matrices à coefficients entiers et de déterminant ± 1. Par exemple, les bases du réseau $\mathbb{Z}^2$ sont exactement les paires de vecteurs $\{(a, b), (c, d)\}$ tels que $a, b, c, d \in \mathbb{Z}$ et $ad - bc = \pm 1$. Ainsi, une autre base de $\mathbb{Z}^2$ est $\{(44341, 38958), (12325, 14028)\}$. Il est clair que cette dernière base est moins agréable que la base canonique $\{(1, 0), (0, 1)\}$. Une particularité de cette dernière est qu'elle est constituée des vecteurs les plus courts du réseau. Un problème fondamental, et pour lequel l'algorithme LLL donne une solution souvent satisfaisante, est, étant donné un réseau défini par une certaine base, de construire une nouvelle base formée de vecteurs courts et aussi orthogonaux que possible. Un tel processus est appelé une réduction du réseau.

Précisons que les transformations que l'on peut effectuer sur une base $(b_1, \ldots, b_n)$ de L, et qui la transforment en une autre base de L, sont exactement les successions de transformations suivantes:

- Changement d'un signe: $b_i \to -b_i$
- Échange de deux vecteurs: $(b_i, b_j) \to (b_j, b_i)$
- Translation: $b_i \to b_i + kb_j$ avec $k \in \mathbb{Z}$, $j \neq i$

À partir d'une base quelconque d'un réseau L, on peut définir un invariant du réseau qui d'appelle le déterminant:

Définition 2. *Une matrice de Gram de L est la matrice des produits scalaires d'une base de L:*

$$G = (b_i \cdot b_j)_{1 \leq i,j \leq n}.$$

Le déterminant du réseau L est le déterminant d'une matrice de Gram de L, et ne dépend pas du choix de la base de L.

Proof. En effet, si G' est la matrice de Gram d'une autre base de L, la matrice de passage P appartient à $GL_n(\mathbb{Z})$ donc est de déterminant ± 1. Comme $G' = P^t G P$, $\det(G') = (\det(P))^2 \det(G) = \det(G)$. Remarquons que, géométriquement, le déterminant de L s'interprète de la façon suivante: $(\det(L))^{1/2}$ est le volume du parallélotope construit sur une base de L:

$$(\det(L))^{1/2} = \mathrm{vol}(\{x = \sum_{i=1}^{n} x_i b_i : 0 \leq x_i \leq 1\}).$$

□

Un réseau L est une partie discrète de $\mathbb{R}^n$ ce qui signifie que, pour tout M, l'ensemble des éléments x de L vérifiant $x \cdot x \leq M$ est fini. Cela nous permet de définir le minimum de L, qui est atteint pour un nombre fini de vecteurs de L.

Définition 3. *Le minimum de L est défini par:*

$$\min(L) = \min\{x \cdot x \mid x \in L \setminus \{0\}\}.$$

L'ensemble des vecteurs minimaux de L est l'ensemble fini

$$S(L) = \{x \in L \mid x \cdot x = \min(L)\}.$$

Les deux quantités $\det(L)$ et $\min(L)$ sont inchangées si on fait agir une transformation orthogonale sur le réseau L. Si on transforme L par une homothétie $x \to \lambda x$, on obtient $\det(\lambda L) = \lambda^{2n} \det(L)$ et $\min(\lambda L) = \lambda^2 \min(L)$. Par conséquent, le quotient

$$\gamma(L) := \frac{\min(L)}{\det(L)^{1/n}}$$

appelé la constante d'Hermite du réseau L, est invariant par les similitudes (composées d'homothéties et de transformations orthogonales). On verra plus loin que ce quotient mesure la densité de l'empilement de sphères associé au réseau L.

Exemples:

(1) $L = \mathbb{Z}^n$. Ce réseau a pour minimum $\min(L) = 1$, et possède $2n$ vecteurs minimaux. De plus $\det(L) = 1$, $\gamma(L) = 1$.
(2) $L = A_2$. On a $\min(L) = 1$, le réseau a 6 vecteurs minimaux; $\det(L) = \begin{vmatrix} 1 & 1/2 \\ 1/2 & 1 \end{vmatrix} = 3/4$, $\gamma(L) = 2/\sqrt{3}$.
(3) Construction de réseaux à l'aide de codes binaires: soit C un code binaire linéaire de paramètres $[n, k, d]$. On définit

$$L_C := \frac{1}{\sqrt{2}}\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : (x_1 \mod 2, \ldots, x_n \mod 2) \in C\}.$$

On montre que $\min(L_C) = \min\{2, d/2\}$ et que $\det(L) = 2^{n-2k}$. Ce procédé permet de construire des réseaux intéressants comme le réseau D_n, associé au code de parité, ou le réseau E_7, de dimension 7, associé au code de Hamming binaire de paramètres $[7, 3, 4]$.

3. Réduction des réseaux en dimension 2

En dimension 2, il existe un algorithme très simple, dû à Gauss, qui permet de réduire un réseau. Cet algorithme, que nous allons décrire, construit une base (b_1, b_2) du réseau, vérifiant la condition suivante, dite de réduction de Gauss: si b_1' complète b_1 en une base orthogonale positive, alors b_2 appartient au domaine

$$D = \{x = \lambda_1 b_1 + \lambda_2 b_1' : |\lambda_1| \leq 1/2 \text{ et } \lambda_2 > 0\}.$$

En outre, si cette condition est réalisée, b_1 est un vecteur minimal de L, comme le montre le lemme:

Lemme 1. *Si $L = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2$ est tel que $b_2 \in D$, alors $\min(L) = b_1 \cdot b_1$. De plus, on est dans l'un des trois cas suivants:*

(1) $S(L) = \{\pm b_1\}$
(2) $S(L) = \{\pm b_1, \pm b_2\}$
(3) $S(L) = \{\pm b_1, \pm b_2, \pm(b_1 + b_2)\}$ *et* $b_1 \cdot b_2 = -1/2$
(i.e. le réseau est hexagonal).

Proof. Supposons $b_1 \cdot b_1 = 1$. Pour $x = x_1 b_1 + x_2 b_2 \in L$, on a $x \cdot x = x_1^2 + 2x_1 x_2 (b_1 \cdot b_2) + x_2^2 (b_2 \cdot b_2)$. Donc $x \cdot x \geq x_1^2 - x_1 x_2 + x_2^2$. L'expression $x_1^2 - x_1 x_2 + x_2^2$ est une forme quadratique définie positive qui prend des

valeurs entières sur les entiers. Donc $x \cdot x \geq 1$. De plus, $x \cdot x = 1$ ne peut être réalisé que si on a les égalités

$$1 = x \cdot x = x_1^2 + 2x_1x_2(b_1 \cdot b_2) + x_2^2(b_2 \cdot b_2) = x_1^2 - x_1x_2 + x_2^2 = 1$$

soit $(x_1, x_2) = (\pm 1, 0), (0, \pm 1)$ ou $\pm(1, 1)$. Ce dernier cas impose en outre que $b_1 \cdot b_2 = -1/2$ et $b_2 \cdot b_2 = 1$ c'est-à-dire que le résequ L est hexagonal. □

L'algorithme de Gauss est le suivant:

> Entrée: Une base (b_1, b_2) de L telle que $b_1 \cdot b_1 \leq b_2 \cdot b_2$
> Sortie: Une base (b_1, b_2) de L vérifiant la condition de réduction de Gauss:
> 1. Remplacer b_2 par $b_2 - \lfloor \frac{b_1 \cdot b_2}{b_1 \cdot b_1} \rceil b_1$
> 2. Si $b_1 \cdot b_1 > b_2 \cdot b_2$, échanger b_1 et b_2 et retourner à l'étape 1.. Sinon, changer éventuellement b_2 en $-b_2$, puis sortir.

Il est clair que, si l'algorithme termine, il sort une base vérifiant la condition de réduction de Gauss.

La preuve que l'algorithme termine repose sur le fait que, à chaque renvoi à 1., la valeur de $b_2 \cdot b_2$ a diminué strictement. Un réseau étant un ensemble discret, elle ne peut prendre qu'un nombre fini de valeurs.

La complexité de cet algorithme est quadratique. Remarquer la similitude avec l'algorithme d'Euclide. Il n'existe pas d'algorithme de réduction aussi simple en dimension supérieure. Par contre l'algorithme LLL est un algorithme de complexité polynomiale, qui construit une base d'un réseau non optimalement réduite mais souvent satisfaisante. Nous allons maintenant étudier cet algorithme.

4. Orthogonalisation de Gram-Schmidt

Soit $\{b_1, \ldots, b_n\}$ une base de $\mathbb{R}^n$. L'orthogonalisation de Gram-Schmidt de cette base est une base de $\mathbb{R}^n$ notée $\{b_1^*, \ldots, b_n^*\}$, qui vérifie les propriétés suivantes:

(1) Elle est orthogonale, i.e. $b_i^* \cdot b_j^* = 0$ si $i \neq j$
(2) Pour tout $i \geq 1$, $\{b_1^*, \ldots, b_i^*\}$ engendre le même sous-espace vectoriel que $\{b_1, \ldots, b_i\}$
(3) (Normalisation) Les deux propriétés précédentes caractérisent les vecteurs b_i^* à multiplication par un scalaire près. Nous imposons en outre que $b_i^* = b_i$ plus une combinaison linéaire des b_j avec $j < i$, ce qui caractérise alors complètement les b_i^*.

Proposition 1. *On a* $b_i = \sum_{j=1}^{i} u_{i,j} b_j^*$ *avec* $u_{i,i} = 1$ *et* $u_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$.

Preuve: D'après la condition 2., il existe des coefficients $u_{i,j}$ tels que

$$b_i = \sum_{j=1}^{i} u_{i,j} b_j^*. \tag{1}$$

La condition 3. équivaut à $u_{i,i} = 1$. Si on calcule le produit scalaire avec b_j^* de cette égalité, puisque les b_j^* sont deux à deux orthogonaux, on trouve

$$b_i \cdot b_j^* = u_{i,j} b_j^* \cdot b_j^*$$

et donc

$$u_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}. \tag{2}$$

□

La proposition précédente permet de calculer les $u_{i,j}$ par récurrence sur i facilement. Posons

$$a_i^2 := b_i^* \cdot b_i^* \text{ avec } a_i > 0.$$

En effet, pour $i = 1$, il n'y a que $u_{1,1} = 1$ ($b_1^* = b_1$) et donc $a_1^2 = b_1 \cdot b_1$. L'équation (2) nous permet de calculer $u_{2,1}$, puis a_2^2 puisque on a $b_2 \cdot b_2 = b_2^* \cdot b_2^* + u_{2,1}^2 a_1^2$, et ainsi de suite.

Réciproquement, en inversant la matrice triangulaire des $u_{i,j}$, on peut calculer les b_i^* en fonction des b_i. Retenons pour usage ultérieur la formule:

$$b_i \cdot b_i = \sum_{j=1}^{i} u_{i,j}^2 a_j^2. \tag{3}$$

4.1. **Interprétation matricielle:** Soit B la matrice dont les colonnes sont les vecteurs b_i, B^* la matrice dont les colonnes sont les vecteurs b_i^*, et A la matrice diagonale dont les coefficients diagonaux sont $a_1, a_2, \ldots, a_n$.

On a : $(B^*)^t B^* = A^2$. Si on pose $K = B^* A^{-1}$, cette matrice vérifie $K^t K = \mathrm{Id}$ et est donc orthogonale. D'autre part, si U est la matrice transposée des $u_{i,j}$, complétée par des zéros en posant $u_{i,j} = 0$ si $i < j$ (U est donc une matrice triangulaire supérieure, avec des 1 sur la diagonale), on a $B = B^* U$, et donc finalement

$$B = KAU$$

(décomposition d'Iwasawa de B).

En particulier, de $B = B^* U$ il vient $G = B^t B = U^t A^2 U$, et, comme la matrice U est de déterminant égal à 1,

$$\det(L) = \prod_{i=1}^{n} a_i^2. \tag{4}$$

4.2. **Application:** l'orthogonalisation de Gram-Schmidt correspond aussi à la "décomposition en somme de carrés" de $x \cdot x$. Elle permet de calculer effectivement l'ensemble $\{x \in L \mid x \cdot x \leq M\}$, et de se convaincre que c'est bien un ensemble fini. En effet, si $x = \sum_{i=1}^{n} x_i b_i \in L$, $x_i \in \mathbb{Z}$:

$$\begin{aligned} x = \sum_{i=1}^{n} x_i b_i &= \sum_{i=1}^{n} x_i \sum_{j=1}^{i} u_{i,j} b_j^* \\ &= \sum_{j=1}^{n} (\sum_{i=j}^{n} x_i u_{i,j}) b_j^* \end{aligned}$$

donc

$$\begin{aligned} x \cdot x &= \sum_{j=1}^{n} (\sum_{i=j}^{n} x_i u_{i,j})^2 a_j^2 \\ &= (x_1 + x_2 u_{2,1} + \dots)^2 a_1^2 + \dots + (x_{n-1} + x_n u_{n,n-1})^2 a_{n-1}^2 + x_n^2 a_n^2 \end{aligned}$$

et la condition $x \cdot x \leq M$ implique:

$$\begin{gathered} -\sqrt{M}/a_n \leq x_n \leq \sqrt{M}/a_n \\ -\sqrt{M}/a_{n-1} - x_n u_{n,n-1} \leq x_{n-1} \leq \sqrt{M}/a_{n-1} - x_n u_{n,n-1} \\ \dots \end{gathered}$$

ce qui conduit à un nombre fini de possibilités pour les valeurs entières de x_n, $x_{n-1}, \dots, x_1$. Il reste à parcourir cet ensemble fini pour finalement déterminer les valeurs de $x_1, \dots, x_n$ pour lesquelles $x \cdot x \leq M$. En particulier, nous avons démontré de façon effective que l'ensemble des vecteurs minimaux $S(L)$ d'un réseau L est fini.

5. Réduction d'Hermite

La condition de réduction de Gauss en dimension 2 peut se traduire en termes de l'orthogonalisation de Gram-Schmidt de la base de la façon suivante:

(1) $|u_{2,1}| \leq 1/2$

(2) $a_2^2 \geq 3/4(a_1^2)$

En dimension quelconque, Hermite démontre qu'un réseau contient toujours une base (dite réduite au sens d'Hermite) vérifiant:

(1) $|u_{i,j}| \leq 1/2$ pout tout $j < i$ (condition de taille)
(2) $a_i^2 \geq 3/4(a_{i-1}^2)$ (condition de quasi orthogonalité)

Malheureusement on ne connait pas d'algorithme polynomial pour construire une telle base en toute dimension... La condition de Lovacz est un relachement de la condition de quasi orthogonalité, qui peut être obtenue par l'algorithme LLL en complexité polynomiale.

6. L'ALGORITHME LLL

LLL=Lenstra, Lenstra, Lovacz (1982) sont les auteurs de cet algorithme. Son application initiale était la factorisation des polynômes à coefficients rationnels.

Définition 4. *Avec les notations du paragraphe précédent, une base* $\{b_1, \ldots, b_n\}$ *d'un réseau* L *est dite* LLL réduite *si elle vérifie les conditions suivantes:*

(1) $|u_{i,j}| \leq 1/2$ *pour tout* $j < i$ *(condition de taille)*
(2) *Pour tout* $i \geq 2$, $a_i^2 \geq (3/4 - u_{i,i-1}^2)a_{i-1}^2$ *(condition de Lovacz)*

Le théorème suivant mesure la "qualité" d'une base LLL-réduite en termes de la norme de ses vecteurs.

Théorème 1. *Soit* $\{b_1, \ldots, b_n\}$ *une base LLL-réduite. Alors:*

(1) $\det(L) \leq \prod_{i=1}^n (b_i \cdot b_i) \leq 2^{\frac{n(n-1)}{2}} \det(L)$
(2) $b_j \cdot b_j \leq 2^{i-1} a_i^2$ *pour tout* $j \leq i$
(3) $b_1 \cdot b_1 \leq 2^{\frac{n-1}{2}} \det(L)^{1/n}$
(4) $b_1 \cdot b_1 \leq 2^{n-1} \min(L)$

Preuve: La relation (3) montre que $b_i \cdot b_i \geq a_i^2$ ce qui montre que

$$\det(L) = \prod_{i=1}^n a_i^2 \leq \prod_{i=1}^n b_i \cdot b_i.$$

Les conditions 1. et 2. de réduction LLL montrent que

$$a_i^2 \geq a_{i-1}^2/2,$$

et donc par induction que

$$a_i^2 \geq a_j^2/2^{i-j}, \text{ pour tout } i > j. \tag{5}$$

En remplaçant dans (3), on obtient

$$b_i \cdot b_i \leq (1 + 1/4(2 + 2^2 + \cdots + 2^{i-1}))a_i^2 = \frac{2^{i-1}+1}{2} a_i^2 \leq 2^{i-1} a_i^2$$

ce qui démontre les points 1. et 2.

D'autre part, $b_1 \cdot b_1 = a_1^2 \leq 2^{i-1} a_i^2$ (par (5)). En multipliant membre à membre, on obtient

$$(b_1 \cdot b_1)^n \leq 2^{\frac{n(n-1)}{2}} \det(L)$$

soit le point 3.

Soit $x \in L$, $x \neq 0$. On peut écrire d'une part $x = x_1 b_1 + \cdots + x_n b_n$ avec les x_i entiers, d'autre part $x = \lambda_1 b_1^* + \cdots + \lambda_n b_n^*$ avec les λ_i réels. Soit i_0 le plus grand indice tel que $\lambda_{i_0} \neq 0$. Alors: $\lambda_{i_0} = x_{i_0}$, et

$$x \cdot x = \lambda_{i_0}^2 a_{i_0}^2 + \sum_{j<i_0} \lambda_j^2 a_j^2 \geq a_{i_0}^2 \geq b_1 \cdot b_1 / 2^{i_0 - 1}$$

où la dernière inégalité se déduit de (5). En prenant $x \in S(L)$ et en utilisant $i_0 \leq n$, on obtient bien l'inégalité du point 4.

Remarque 1. *Dans la pratique, la norme des vecteurs obtenus par réduction LLL est meilleure que la borne théorique du théorème précédent. Nous allons maintenant décrire cet algorithme.*

Algorithme LLL:. il prend en entrée une base $\{b_1, \ldots, b_n\}$ d'un réseau L, et sort une base $\{b'_1, \ldots, b'_n\}$ de ce même réseau, LLL-réduite.

Supposons que les $k-1$ premiers vecteurs $b_1, b_2, \ldots, b_{k-1}$ vérifient les conditions de réduction LLL. On suppose avoir calculé les coefficients $u_{i,j}$ pour $j \leq i \leq k-1$ ainsi que les a_i^2 pour $1 \leq i \leq k-1$.

On s'occupe d'abord de la condition 1., qui est facile à obtenir. En effet, supposons que l'on remplace le vecteur b_k par un vecteur de la forme $b_k - q b_l$ avec $l < k$ et q entier. Alors:

- Le réseau engendré par $b_1, \ldots, b_k$ reste le même
- L'orthogonalisation de Gram-Schmidt $b_1^*, \ldots, b_k^*$ reste la même
- Les coefficients $u_{k,k}, \ldots, u_{k,l+1}$ sont inchangés; $u_{k,l}$ est remplacé par $u_{k,l} - q$.

Le dernier point est conséquence de l'égalité: $b_k - q b_l = \sum_{j=1}^{k} (u_{k,j} - q u_{l,j}) b_j^*$. Ainsi, on voit que l'on peut obtenir successivement les conditions: $|u_{k,k-1}| \leq 1/2$ en remplaçant b_k par $b_k - \lfloor u_{k,k-1} \rceil b_{k-1}$, puis $|u_{k,k-2}| \leq 1/2$ en remplaçant b_k par $b_k - \lfloor u_{k,k-2} \rceil b_{k-2}$, et ainsi de suite.

RED(k,l) est la procédure qui remplace b_k par $b_k - \lfloor u_{k,l} \rceil b_l$, et met à jour les coefficients $u_{k,j}$ pour $j \leq l$.

Ainsi, pour obtenir la condition 1., il faut exécuter successivement RED(k,k-1), RED(k,k-2), jusqu'à RED(k,1). Mais il faut remarquer que la condition 2. peut être testée dès que RED(k,k-1) est exécutée, puisque ensuite le coefficient $u_{k,k-1}$ ne bouge plus.

On procède donc de la façon suivante: on exécute RED(k,k-1), puis, juste après, on teste la condition 2. Si elle est vérifiée, on exécute RED(k,k-2), ..., RED(k,1) puis on passe bien sûr au vecteur suivant b_{k+1}.

Si elle n'est pas vérifiée: on échange b_k et b_{k-1} et on redescend au cran précédent. Remarquer qu'après cet échange, on a toujours une base de L. Par contre, seulement les $k-2$ premiers vecteurs sont LLL-réduits. D'autre part, b^*_{k-1} est modifié.

SWAP(k) est la procédure qui échange b_{k-1} et b_k, et met à jour les b^*_i et les coefficients $u_{i,j}$. Les vecteurs $b^*_1, \ldots, b^*_{k-2}$ n'ont pas bougé, ni les $u_{i,j}$ pour $i \leq k-2$. Comme

$$b_k = b^*_k + u_{k,k-1}b^*_{k-1} + u_{k,k-2}b^*_{k-2} + \ldots,$$

b^*_{k-1} est remplacé par $b^*_k + u_{k,k-1}b^*_{k-1}$, et les coefficients $u_{k-1,j}$ par $u_{k,j}$ pour $j < k-1$.

Preuve de l'algorithme: Il est clair que, si cet algorithme termine, il sort bien une base LLL-réduite.. Ce qui n'est pas du tout évident, c'est qu'il termine bien, c'est-à-dire qu'il ne poursuit pas indéfiniment une succession de montées et de descentes dans les indices de 1 à n. Il faut donc démontrer qu'il ne passe par la procédure SWAP qu'un nombre fini de fois.

Posons $L_k = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_k$ et $D_k = \det(L_k)$. On a, en vertu de (4), $D_k = \prod_{i=1}^{k} a_i^2$. La valeur prise par le n-uplet $(D_1, D_2, \ldots, D_n)$ ne change que dans la procédure SWAP. Lors de l'échange de b_{k-1} et b_k, les réseaux L_1,...,L_{k-2} sont inchangés, ainsi que L_k,...,L_n. Seul L_{k-1} est modifié. Plus précisément, on garde b^*_1,...,b^*_{k-2}, et b^*_{k-1} devient ${b'_{k-1}}^* = b^*_k + u_{k,k-1}b^*_{k-1}$, donc a^2_{k-1} devient ${a'_{k-1}}^2 = a^2_k + u^2_{k,k-1}a^2_{k-1}$. Donc D_{k-1} est remplacé par

$$D'_{k-1} = D_{k-1}\frac{a^2_k + u^2_{k,k-1}a^2_{k-1}}{a^2_{k-1}}.$$

Mais justement, si on passe dans SWAP, c'est parce que la condition 2. de réduction LLL n'est pas vérifiée, c'est-à-dire parce que

$$a^2_k < (3/4 - u^2_{k,k-1})a^2_{k-1},$$

soit

$$\frac{a^2_k + u^2_{k,k-1}a^2_{k-1}}{a^2_{k-1}} < \frac{3}{4}.$$

On a donc: $D'_{k-1} < \frac{3}{4}D_{k-1}$.

Ainsi, chaque passage par SWAP multiplie le produit $D_1 D_2 \dots D_n$ par un facteur au plus égal à $3/4$. Il suffit donc de montrer que ce produit est minoré par une constante ne dépendant que du réseau L.

Proposition 2. *Si L est un réseau de dimension n, le quotient*

$$\gamma(L) := \frac{\min(L)}{\det(L)^{1/n}}$$

est majoré par une constante ne dépendant que de n.

Preuve: En effet, ce quotient mesure la densité Δ de l'empilement de sphères associé à L. Soit $r = \sqrt{\min(L)}/2$. Les sphères de centre les points du réseau L et de rayon r sont d'intérieurs disjoints (c'est le plus grand rayon possible..). Soit $\mathcal{E}$ la réunion de ces sphères et soit $\mathcal{P}$ le parallélotope construit sur une base $\{b_1, \dots, b_n\}$:

$$\mathcal{P} = \{x_1 b_1 + \dots + x_n b_n \mid 0 \leq x_i \leq 1\}.$$

Le volume de $\mathcal{P}$ est égal à $\sqrt{\det(L)}$. Le volume de $\mathcal{P} \cap \mathcal{E}$ est égal au volume d'une sphère de rayon r, c'est-à-dire à $r^n \pi_n$ où π_n est le volume de la sphère de rayon 1 et de dimension n. On a bien sûr

$$\Delta = \frac{\mathrm{vol}(\mathcal{P} \cap \mathcal{E})}{\mathrm{vol}(\mathcal{P})} \leq 1$$

soit

$$\frac{r^n \pi_n}{\sqrt{\det(L)}} \leq 1$$

ou encore

$$\left(\frac{\min(L)}{\det(L)^{1/n}}\right)^{n/2} \frac{\pi_n}{2^n} \leq 1.$$

□

Terminons maintenant la démonstration de l'algorithme LLL: La proposition précédente montre que

$$\gamma_k := \sup_{L \subset \mathbb{R}^k} \gamma(L)$$

est fini. On a donc, pour les réseaux L_k,

$$D_k \geq \left(\frac{\min(L_k)}{\gamma_k}\right)^k \geq \left(\frac{\min(L)}{\gamma_k}\right)^k$$

et le produit $D_1 \dots D_n$ est bien minoré par une constante positive ne dépendant que du réseau L.

□

7. APPLICATIONS

L'algorithme LLL permet de résoudre des problèmes, qui peuvent se ramener à la recherche de petits vecteurs dans un réseau. Initialement, les trois auteurs ont obtenu grâce à lui un algorithme polynomial pour la factorisation des polynômes à coefficients entiers. Nous décrivons maintenant quelques applications de LLL à la cryptographie.

7.1. **Le problème du sac à dos.**

L'un des premiers cryptosystèmes à clé publique proposé était basé sur le problème du sac à dos. Proposé par Merkle et Hellmann en 1978, Ce système a été "cassé" par l'algorithme LLL.

Soit $a_1, a_2, \dots, a_n$ et s des nombres entiers positifs. Il s'agit de répondre à la question:

Existe-t-il un sous-ensemble $I \subset \{1, \dots, n\}$ tel que $s = \sum_{i \in I} a_i$?

Ce problème est connu pour être NP-complet. Cela signifie que tout problème NP peut se réduire à celui-ci. En particulier, comme on pense que NP $\neq$ P, il n'aurait pas de solution polynomiale. Toutefois, il existe des cas particuliers pour lesquels il est très facile de répondre - on parle d'instances faibles.

Définition 5. *On dit que le sac à dos est à super-croissance si* $a_j > \sum_{i=1}^{j-1} a_i$ *pour tout* j.

Dans ce cas, il est trivial de reconnaitre si un entier s donné est ou non la somme d'un sous-ensemble des a_i. En effet, il suffit de procéder de la façon suivante (appelée *algorithme glouton*):

- Déterminer le plus grand des a_i tel que $a_i \leq s$
- Remplacer s par $s - a_i$
- Recommencer tant que s n'est pas plus petit que tous les a_i.

Si, à la fin de la procédure, $s \neq 0$ c'est que s ne se décompose pas en sous-somme des a_i; sinon, c'est qu'on a effectivement trouvé une telle décomposition.

En effet, si $s = a_{i_1} + a_{i_2} + \dots a_{i_s}$, avec $a_{i_1} < a_{i_2} < \dots < a_{i_s}$, on a bien $a_{i_s} \leq s$, et $s \leq \sum_{i=1}^{i_s} a_i < a_{i_s+1}$. Donc $a_{i_s} \leq s < a_{i_s+1}$, et a_{i_s} est bien le plus grand des a_i plus petits que s. Noter que, dans le cas d'un sac à dos à super-croissance, la décomposition si elle existe est unique.

Le cryptosystème proposé par Merkle et Hellmann est le suivant: Alice veut envoyer un message confidentiel à Bob. Bob choisit un sac à

dos à super-croissance $a_1, \ldots, a_n$ ainsi que w et m, avec $m > \sum_{i=1}^n a_i$, et $(w, m) = 1$. Il calcule $b_i = a_i w \mod m$.

- La clé publique est: $b_1, b_2, \ldots, b_n$
- La clé privée est: m, w.

Lorsque Alice veut envoyer un message $\epsilon_1, \ldots, \epsilon_n$ avec $\epsilon_i = 0, 1$ à Bob, elle calcule $s := \sum_{i=1}^n \epsilon_i b_i$ et envoit s à Bob. Bob calcule sw^{-1} modulo m, puis résoud $sw^{-1} = \sum_{i=1}^n \epsilon_i a_i$ suivant l'algorithme glouton. Un attaquant est confronté au pb de résoudre $s = \sum_{i=1}^n \epsilon_i b_i$ pour le sac à dos donné par $b_1, \ldots, b_n$ qui n'est plus à croissance rapide. Merkle et Hellmann proposent comme choix de paramètres $a_1 \simeq 2^n, a_2 \simeq 2^{n+1}, \ldots, a_n \simeq 2^{2n}$.

Lagarias et Odlysko ont montré comment utiliser LLL pour résoudre une certaine famille de sac à dos: les sac à dos de basse densité.

Définition 6. *La densité d'un sac à dos $a_1, a_2, \ldots, a_n$ est la valeur $d = n/\log(\max(a_i, 1 \leq i \leq n))$.*

À $a_1, a_2, \ldots, a_n, s$ on associe le réseau L de dimension $n+1$ de $\mathbb{R}^{n+2}$ engendré par les lignes de la matrice:

$$B = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & Ka_1 \\ 0 & 1 & \ldots & 0 & 0 & Ka_2 \\ \vdots & & & & \vdots & \\ 0 & 0 & \ldots & 1 & 0 & Ka_n \\ 0 & 0 & \ldots & 0 & 1 & -Ks \end{pmatrix}$$

Si on note $e_1, e_2, \ldots e_{n+1}$ les lignes de B, et si $x = \sum_{i=1}^{n+1} x_i e_i \in L$, on a

$$x \cdot x = x_1^2 + x_2^2 + \cdots + x_{n+1}^2 + K^2(x_1 a_1 + \cdots + x_n a_n - x_{n+1} s)^2.$$

Une solution du sac à dos $s = \sum_{i=1}^n \epsilon_i a_i$ correspond à un vecteur $x = \epsilon_1 e_1 + \cdots + \epsilon_n e_n + e_{n+1} = (\epsilon_1, \ldots, \epsilon_n, 1, 0)$ appartenant à L, avec $x \cdot x = \text{card}\{i | \epsilon_i = 1\} + 1 \leq n+1$. Quitte à changer s en $\sum_{i=1}^n a_i - s$, on peut même se ramener à $x \cdot x \leq (n+1)/2$. Si on choisit K tel que $K^2 > (n+1)/2$, tout vecteur $x = \sum_{i=1}^n x_i e_i$ de L vérifiant $x \cdot x \leq (n+1)/2$ est tel que: $x_1 a_1 + \cdots + x_n a_n = x_{n+1} s$. L'idée est donc de rechercher par LLL des vecteurs de petite norme dans ce réseau, qui auront de bonnes chances de fournir une solution au sac à dos.

Plus rigoureusement, on peut montrer que, si le sac à dos est de basse densité, la probabilité d'existence d'un vecteur du réseau de norme inférieure à $(n+1)/2$, qui n'est pas une solution du sac à dos (i.e. dont le coefficients ne sont pas des 0 et des 1), tend vers 0 quand n tend vers $+\infty$.

7.2. **RSA petit exposant: l'attaque de Coppersmith.** ... A compléter.....

8. Autres applications cryptographiques des réseaux

.... A compléter .....

9. Appendice: Sous-groupes discrets de $\mathbb{R}^n$

Dans ce paragrapphe, on montre l'équivalence entre les notions de réseau, tels que définis ici, et de sous-groupe discret de $\mathbb{R}^n$. Rappelons que le rang d'un sous-ensemble de $\mathbb{R}^n$ est la dimension du $\mathbb{R}$-espace vectoriel engendré par cet ensemble. D'un ensemble de rang n, on peut toujours extraire une $\mathbb{R}$-base (mais pas une $\mathbb{Z}$-base!).

Théorème 2. *Soit L un réseau de $\mathbb{R}^n$; alors L est un sous-groupe discret de $\mathbb{R}^n$. Réciproquement, soit L un sous-groupe discret de $\mathbb{R}^n$, non contenu dans un sous-espace vectoriel strict de $\mathbb{R}^n$ (i.e. de rang n). Alors L possède une Z-base qui est aussi une base de $\mathbb{R}^n$, i.e. L est un réseau au sens de la définition 1.*

Preuve: On a démontré au paragraphe précédent que $\{x : x \in L \mid x \cdot x \leq M\}$ est un ensemble fini. Cela montre bien que 0 est isolé dans L. Plus généralement, la même démonstration, en remplaçant x par $x - y$ avec $x \in L$, $y \in \mathbb{R}^n$, montre que l'intersection $L \cap B(y, M)$ est finie. Remarquons qu'il n'est pas vrai qu'un sous-groupe de $\mathbb{R}^n$ est toujours discret. Par exemple, le $\mathbb{Z}$-sous-module de $\mathbb{R}$ engendré par 1 et π (ou 1 et n'importe quel nombre irrationnel) contient une infinité d'éléments dans l'intervalle $]0, 1[$: par exemple $\{n\pi - [n\pi] : n \in \mathbb{N}\}$.

Réciproquement, soit L un sous-groupe discret de $\mathbb{R}^n$. Supposons d'abord $n = 1$. Pour tout intervalle compact $[a, b]$, l'ensemble $L \cap [a, b]$ est fini. On peut en déduire que $L \cap \mathbb{R}^{*+}$ possède un plus petit élément a. On a bien sûr $a\mathbb{Z} \subset L$. Montrons que $L = a\mathbb{Z}$: pour tout élément $x \in L$, il existe un entier k tel que $ka \leq x < (k+1)a$. Alors $0 \leq x - ka < a$; mais $x - ka \in L$ et a est le plus petit élément positif de L. Donc $x - ka = 0$.

Nous allons maintenant considérer le cas général, et construire par récurrence une $\mathbb{Z}$-base de L. Tout d'abord, observons que L contient nécessairement une $\mathbb{R}$-base. En effet, on peut définir une suite emboitée de sous-espaces vectoriels $V_1 \subset V_2 \subset \cdots \subset V_k$ en posant $V_k =$ le sous-espace vectoriel engendré par l'ensemble (fini) $\{x \in L \mid x \cdot x \leq k\}$. En considérant la suite des dimensions de V_k, qui est une suite croissante d'entiers entre 0 et n, on conclut que, soit il existe un entier k_0 à partir duquel $V_k = \mathbb{R}^n$, et dans ce cas on peut extraire de $\{x \in L \mid x \cdot x \leq k_0\}$ une base de $\mathbb{R}^n$ formée de vecteurs de L, soit la suite V_k est stationnaire à un sous-espace W strict de $\mathbb{R}^n$. Dans ce cas, $L \subset W$ ce qui contredit l'hypothèse.

Soit donc $\{e_1, e_2, \ldots, e_n\}$ une $\mathbb{R}$-base contenue dans L. Bien sûr, il n'y a pas de raisons pour que ces vecteurs forment une $\mathbb{Z}$-base de L. Soit W le

sous-espace vectoriel de $\mathbb{R}^n$ engendré par $\{e_1, e_2, \ldots, e_{n-1}\}$. Clairement, W est de dimension $n-1$; soit ϵ_n une base de $W^\perp$. Soit $M := L \cap W$. Alors M est un sous-groupe de W, qui est discret dans W puisque L l'est. En identifiant W et $\mathbb{R}^{n-1}$, on peut trouver par récurrence une base $\{b_1, b_2, \ldots, b_{n-1}\}$ de M, qui soit une $\mathbb{R}$-base de W. D'autre part, tout élément $x \in L$ s'écrit $x = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + \lambda_n \epsilon_n$. Les λ_i ne sont pas des entiers à priori. Considérons

$$\Lambda := \{\lambda \in \mathbb{R} \mid \text{ il existe } x \in L \mid x = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + \lambda \epsilon_n\}.$$

Clairement, Λ est un sous-groupe de $\mathbb{R}$; montrons qu'il est discret. Supposons par l'absurde que $\Lambda \cap [a,b]$ soit infini. Chaque $\lambda \in \Lambda \cap [a,b]$ est associé à un $x \in L$ avec $x = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + \lambda \epsilon_n$. Quitte à soustraire $[\lambda_i] b_i$, qui appartient à L, on peut se ramener à $0 \leq \lambda_i < 1$. Alors x appartient à un ensemble compact K; on aurait donc $K \cap L$ infini, ce qui contredit l'hypothèse suivant laquelle L est discret. On peut donc conclure qu'il existe $a > 0$ tel que $\Lambda = a\mathbb{Z}$ (c'est le cas $n = 1$). Soit alors $b_n \in L$ tel que

$$b_n = \lambda_1 b_1 + \cdots + \lambda_{n-1} b_{n-1} + a\epsilon_n. \tag{6}$$

Nous allons montrer que $\{b_1, b_2, \ldots, b_n\}$ est une base de L. D'abord, par construction, $\{b_1, b_2, \ldots, b_n\}$ forme une famille libre sur $\mathbb{R}$, donc à fortiori sur $\mathbb{Z}$. Il reste à montrer qu'elle engendre L. Soit donc $x \in L$ quelconque. On peut écrire x comme combinaison linéaire des b_i *à coefficients réels*; $x = x_1 b_1 + \cdots + x_n b_n$. En remplaçant b_n par son expression (6), on voit que $x_n a \in \Lambda = a\mathbb{Z}$, donc que $x_n \in \mathbb{Z}$. Alors $y := x - x_n b_n$ appartient à $M = L \cap W$, donc on a aussi $x_1, \ldots, x_{n-1} \in \mathbb{Z}$.

□

Corollaire 1. *Si L est un réseau de $\mathbb{R}^n$, tout sous-$\mathbb{Z}$-module M contenu dans L et de rang n est un réseau. En particulier, M possède une $\mathbb{Z}$-base.*

Si L et M sont deux réseaux de $\mathbb{R}^n$, tels qu'il existe un entier k tel que $kM \subset L$, alors $L \cap M$ et $L + M$ sont aussi des réseaux.

Preuve: Si $M \subset L$ et si L est un réseau, alors M est discret. La première assertion résulte directement du théorème précédent.

Les inclusions $kM \subset L \cap M \subset M$ montrent que d'une part $L \cap M$ est de rang n et d'autre part est un sous-module de L. Donc $L \cap M$ est un réseau.

Montrons maintenant qu'il existe un entier l tel que $L + M \subset \frac{1}{l} M$, et par le même argument on pourra conclure que $L + M$ est un réseau. Choisissons une base $e_1, \ldots, e_n$ de L et une base $f_1, \ldots, f_n$ de M. Soit P la matrice de passage exprimant $f_1, \ldots, f_n$ sur $e_1, \ldots, e_n$. Comme $kM \subset L$,

la matrice kP est à coefficients entiers. Donc la matrice P^{-1} est à coefficients rationnels. Il existe un entier l tel que lP^{-1} soit à coefficients entiers; alors $lL \subset M$, et $L + M \subset \frac{1}{l}M$.

□