M2 CRYPTO
TD THÉORIE ALGORITHMIQUE DES NOMBRES

CHRISTOPHE RITZENTHALER

1. Réseaux

Exercice 1. Une matrice $M \in M_d(\mathbb{Z})$ est dite *unimodulaire* si son déterminant vaut ± 1.

(1) Montrer que M est inversible et que M^{-1} est unimodulaire.

(2) Montrer que si $d = 2$ alors M est égale à $\pm Id$ ou $\pm \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ fois un produit (ou des inverses) de $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ et $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

(3) Montrer que (b_i) et (c_i) sont deux bases d'un même réseau si et seulement si il existe une matrice unimodulaire M telle que $M(b_i) = (c_i)$.

Exercice 2. Soit L un réseau de dimension d. Montrer que le nombre de vecteurs $x \in L$ tels que $||x|| = \lambda$ est minimale et non nulle est majoré par 3^d. Ce nombre s'appelle *kissing number*. On pourra regarder le volume des boules ouvertes centrées en ces points et de rayon $\lambda/2$.

Exercice 3. Le but de l'exercice est de montrer que tout réseau Λ de dimension n a au plus $2^{O(n^3)}$ bases réduites.

(1) **(0,5)** Soit λ la distance minimale de Λ et $(b_1, \dots, b_n)$ une base réduite. Montrer que $||b_1|| \leq r$ avec $r = 2^{O(n)}\lambda$.

(2) **(1)** En considérant la sphère de rayon r et les sphères de rayons $\lambda/2$, montrer qu'il y a au plus $2^{O(n^2)}$ points du réseau de longueur inférieure ou égale à r. Conclure sur le nombre de possibilités pour b_1.

(3) **(2)** On considère maintenant la projection $((b'_2, \dots, b'_n)$ des vecteurs $(b_2, \dots, b_n)$ sur l'orthogonal à b_1. Montrer que $(b'_2, \dots, b'_n)$ forment encore une base réduite (pour le réseau engendré par $(b'_2, \dots, b'_n)$).

(4) **(1,5)** Montrer que b'_2 ne peut provenir que d'au plus deux b_2 d'une base réduite de Λ dont le b_1 est fixé.

(5) **(1)** En déduire que le nombre de b_2 possibles est au plus $2^{O((n-1)^2)}$.

(6) **(1)** Conclure par récurrence le résultat annoncé.

Exercice 4. Soit L un réseau de dimension d.

(1) En utilisant le théorème de Minkowski avec un parallélépipède, montrer qu'il existe un x non nul dans L tel que $||x||_\infty \leq (\det L)^{1/d}$.

(2) Montrer que pour ce x on a $||x||_2 \leq \sqrt{d}(\det L)^{1/d}$.

On va maintenant donner un résultat moins fort mais constructif. Soit $b_1^* = b_1$ et $b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*$.

(3) Montrer par récurrence qu'on pourra toujours prendre $|\mu_{i,i-1}| \leq 1/2$ quitte à remplacer b_i par $b'_i = b_i - \lfloor \mu_{i,i-1} \rceil b_{i-1}$.

(4) Montrer que la condition $||b_{i-1}^*||_2 \leq ||b_i^* + \mu_{i,i-1} b_{i-1}^*||_2$ s'interprète géométriquement en terme de la projection de b_{i-1} et de b_i sur $\langle b_1, \ldots, b_{i-2} \rangle^\perp$.

(5) En déduire que quitte à échanger b_{i-1} et b_i, la propriété ci-dessus est vraie.

On voudrait obtenir simultanément les deux propriétés. On considère l'algorithme ci-dessous

Algorithm 1: Procédure réduction

Rendre tous les $\mu_{i,i-1}$ inférieurs à $1/2$ en valeur absolue.
while $\exists i_0, ||b_{i_0-1}^*||_2 > ||b_{i_0}^* + \mu_{i_0,i_0-1} b_{i_0-1}^*||_2$ **do**
  échanger b_{i_0} et b_{i_0-1}
  rendre tous les $\mu_{i,i-1}$ inférieurs à $1/2$ en valeur absolue.

(6) Montrer que l'algorithme finit car les $(||b_1^*||_2, \ldots, ||b_d^*||_2)$ décroissent strictement à chaque itération pour l'ordre lexicographique.

(7) montrer que pour $i > 1$ on a $3/4||b_{i-1}^*||_2^2 \leq ||b_i^*||_2^2$ à la fin de l'algorithme.

(8) En utilisant le fait que $\det L = \prod ||b_i^*||_2$, montrer la borne d'Hermite

$$||b_1||_2 \leq (\sqrt{4/3})^{(d-1)/2} \det(L)^{1/d}.$$

Exercice 5. On considère le réseau L engendré par les colonnes de

$$\begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

On considère $b_4' = 2b_4 - b_1 - b_2 - b_3$. Montrer que b_1, b_2, b_3, b_4' son linéairement indépendants et qu'ils atteignent la longueur minimale 2 mais qu'il n'engendrent pas le réseau L.
En dimension ≥ 5, il existe des réseaux pour lesquelles aucun choix de vecteurs atteignant les minimaux ne forment une base du réseau.

Exercice 6. En dimension 2, on considère l'algorithme suivant (où $q(u) = ||u||^2$). On

Algorithm 2: Algorithme de Gauss

input : Une base ordonnée $(u.v)$ avec $q(u) \leq q(v)$
output: Une base réduite du réseau
repeat
  $x = \lfloor (u, v)/q(u) \rceil$
  $r = v - xu$
  $v = u$
  $u = r$
until $q(u) \geq q(v)$;
return (v, u)

s'occupe d'abord de la correction de l'algorithme.

(1) Montrer que la sortie (U, V) est bien une base du réseau.

(2) Montrer que $q(U) \leq q(V)$ et que pour tout $y \in \mathbb{Z}$ on a $q(V + yU) \geq q(V)$.

(3) En utilisant alors que $q(U + V) \geq q(V)$ et que $q(U - V) \geq q(V)$ en déduire que $|(U, V)| \leq q(U)/2$.

(4) Montrer que $q(U)$ est minimale en montrant que si $q(x_1U + x_2V) < q(U)$ alors $x_1 = x_2 = 0$.

(5) Montrer que $q(V)$ atteint le second minimum, i.e. que $q(x_1U + x_2V) < q(V)$ avec $x_2 \neq 0$ n'est pas possible.

On s'intéresse maintenant au temps d'exécution.

(6) Montrer que si $x = 0$ alors la boucle est terminée.

(7) Montrer que $|x| = 1$ n'est possible qu'aux deux premières ou à la dernière itération de l'algorithme (on raisonnera par l'absurde en montrant que r n'est pas alors le choix minimal).

(8) On suppose donc $|x| > 1$. Montrer qu'alors $|(u, v)|/q(u) \geq 3/2$.

(9) Soit $v^\perp$ la projection de v sur $\langle u\rangle^\perp$. Montrer que $q(v) \geq q(v^\perp) + 9/4q(u)$.

(10) Montrer que $q(r) \leq q(v^\perp) + 1/4q(u)$.

(11) En déduire que $q(v) \geq q(r) + 2q(u)$, puis que si on n'est pas à la dernière itération alors $q(v) \geq 3q(r)$.

(12) En déduire que sauf au deux premières ou à la dernière itération alors $q(u)q(v)$ décroît d'un facteur 3 à chaque itération. Si on note λ_1 le minimum du réseau et u_0, v_0 les vecteurs d'entrée, montrer que le nombre d'itérations est au plus $2\log_3 q(v_0)/\lambda_1^2 + 2 = O(\log q(v_0))$.

(13) Le coût des étapes internes à la boucle est majoré par le coût du calcul de x qui est une division euclidienne. Si on écrit $a = bq + r$ alors le coût est $O(\log(a)^2)$. En déduire le coût total de l'algorithme.

2. Solutions

1 (1) On utilise le fait que $M^{-1} = 1/det(M) \cdot {}^tM^{\text{co}}$ et que la comatrice est à coeffcients entiers puisque ce sont des déterminants extraits de M.

(2) Notons J la première matrice et T la seconde. On a clairement $T^b = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. D'autre part $T' = JTJ = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Si on part d'une matrice $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ alors $M - T^{\lfloor b/a \rfloor}$ remplace le coefficient b par le reste de la division euclidienne de b par a. En appliquant alors J, on intervertit la place du reste et de a. On peut ainsi effectuer une division euclidienne et obtenir in fine un 0 à la place de b. On raisonne de même avec T' (la ligne du haut reste alors inchangée) et on obtient ainsi une matrice diagonale de déterminant ± 1.

(3) Si les (b_i) et les (c_i) engendrent le même réseau alors il existe une matrice M à coefficients entiers telle que $M(b_i) = (c_i)$ et une matrice N telle que $N(c_i) = (b_i)$. Mais alors $NM(b_i) = (b_i)$ et comme la matrice des (b_i) est inversible $MN = Id$ donc M est unimodulaire. La réciproque est immédiate.

2 Soit X l'ensemble des vecteurs de norme λ et considérons les boules ouvertes centrées en les points de X de rayon $\lambda/2$. Ces boules sont disjointes : en effet la distance entre deux points quelconque du réseau est plus grande que λ (sinon en translatant, on aurait un vecteur de norme plus petite). Elles sont de plus incluses dans la boule de centre 0 et de rayon $3\lambda/2$. Ainsi

$$\#X \leq \frac{\text{vol(boule de rayon } 3\lambda/2)}{\text{vol(boule de rayon } \lambda/2)} = 3^d.$$

3 (1) C'est le cours : $||b_1|| \leq \sqrt{2}^{(n-1)}\lambda$

(2) Les boules étant disjointes et centrées en N points on a que $N \cdot c \cdot (\lambda/2)^n \leq c \cdot (r + \lambda/2)^n$. D'où $N \leq (1 + 2r/\lambda)^n \leq 2^{O(n^2)}$.

(3) La base de départ est propre, i.e. $b_i^* = b_i - \sum \mu_{ij} b_j^*$. Mais les nouveaux $b_i' = b_i - \mu_{i1} b_1^*$. Ainsi les $b_i'^*$ sont les mêmes que les b_i^* et les μ_{ij} aussi. La base est donc propre et la condition Siegel réduite est bien sûr respectée.

(4) En faisant un dessin dans le plan b_1, b_2, si un vecteur c_2 a la même image que b_2 sur l'orthogonal à b_1, il doit s'écrire $b_2 + mb_1$. Si on veut qu'il soit réduit on doit avoir

$$\frac{\langle c_2, b_1 \rangle}{||b_1||^2} = m + \mu_{12}$$

qui doit être inférieur à $1/2$ Cela ne peut arriver que pour $m = 0$ et ($m = -1$ si $\mu_{12} = 1/2$) et ($m = 1$ si $\mu_{12} = -1/2$). Donc au plus 2 solutions.

(5) On s'est ramené à raisonner sur b_2' dont le nombre est majoré par $2^{O((n-1)^2)}$ par le même argument que pour b_1. C'est aussi le nombre de b_2.

(6) On a donc au plus $\prod_{i=1}^{n} 2^{O(i^2)} = 2^{O(n^3)}$.

4 (1) Prenons $S = [-\det(L)^{1/d}, det(L)^{1/d}]$ et on utilise le deuxième théorème de Minkowski. On a $vol(S) = 2^d \det(L)$ et donc il existe $x \in (L \setminus \{0\}) \cap S$. Donc $||x||_\infty \leq (\det L)^{1/d}$.

(2) On a $||x||_2^2 \leq \sum_{i=1}^{d} ||x||_\infty^2 \leq d||x||_\infty^2$.

(3) Pour $i = 1$ la condition est vide (et donc satisfaite). On suppose par récurrence que pour tout $i \in \{2, \ldots, k-1\}$ on a $|\mu_{i,i-1}| \leq 1/2$. Si $|\mu_{k,k-1}| \leq 1/2$ alors c'est gagné. Sinon, on pose $b_k' = b_k - \lfloor \mu_{k,k-1} \rceil b_{k-1}$. La base $B' = (b_1, \ldots, b_{k-1}, b_k', b_{k+1}, \ldots, b_d)$ est encore une base de L. De plus $\mu_{ij}' = \mu_{ij}$ pour tout $j < i < k$. Il suffit maintenant de majorer

$$\mu_{k,k-1}' = \frac{b_k', b_{k-1}}{q(b_{k-1})} = \mu_{k,k-1} - \lfloor \mu_{k,k-1} \rceil.$$

D'où le résultat.

(4) Cela signifie que la projection de b_{i-1} (qui vaut b_{i-1}^*) est plus courte que la projection de $b_i = b_i^* + \mu_{i,i-1} b_{i-1}^* + \sum_{j<i-2} \mu_{ij} b_j^*$ qui vaut bien $b_i^* + \mu_{i,i-1} b_{i-1}^*$ (ce vecteur est bien orthogonal au sous-espace engendré par les $b_1, \ldots, b_{i-2}$ et b_i s'exprime comme ce vecteur plus un élément du sous-espace).

(5) En effet, cela ne change pas le sous-espace et on a donc bien le résultat.

(6) On a vu que la réduction des $\mu i, j$ ne change pas la GSO. Donc s'il y a un changement c'est lors de l'échange de b_{i_0-1} avec b_{i_0} qui devient le nouveau b_{i_0-1}. Les vecteurs de la GSO sont inchangés jusqu'à $i_0 - 2$ et celui en i_0 devient $b_{i_0}^* + \mu_{i,i-1} b_{i_0-1}^*$ qui est plus court par hypothèse que l'ancien b_{i_0-1}. On a donc une décroissance à chaque étape dans l'ordre des vecteurs. Mais $||b_1 * || = ||b_1||$ pour un vecteur du réseau b_1 et en particulier est supérieure à $\lambda(L)$. On ne peut donc pas avoir une décroissance infinie et l'algorithme s'arrête (rem. on est dans le cas $\delta = 1$ de LLL : l'algorithme n'est plus forcément en temps polynomiale).

(7)

$$q(b_{i-1}^*) \leq q(b_i^*) + |\mu_{i,i-1}|^2 q(b_{i-1}^*) \leq q(b_i^*) + 1/4 q(b_{i-1}^*).$$

D'où le résultat en regroupant les $q(b_{i-1}^*)$.

(8)
$$\det(L) = \prod_{i \leq d} ||b_i^*||_2 \geq \prod ||b_1||_2 (\sqrt{3/4})^{i-1} \geq ||b_1||_2^d (\sqrt{3/4})^{d(d-1)/2}.$$

5 Tout est clair sauf que le minimum est 2. Or un vecteur du réseau s'écrit $(2a+d, 2b+d, 2c+d, d)$ qui ne peut être de norme 1 (distinguer le cas $d=0$, $|d| \geq 2$ et le cas $|d|=1$ pour lequel $(2a+d)^2, (2b+d)^2, (2c+d)^2$ et d^2 sont impaires, donc ≥ 1 donc leur somme plus grande que 4.

6 (1) (U, V) est bien une base car elle est obtenue à partir de (u, v) par des opérations élémentaires, inversibles à coefficients entiers.

(2) La condition de sortie nous donne $q(U) = q(v_f) \leq q(u_f) = q(V)$ où (u_f, v_f) sont les u, v à la fin de l'algorithme. Pour la seconde condition, on a $q(V + yU) = q(u_f + yv_f) = q(v_{f-1} - xu_{f-1} + yu_{f-1}) = q(v_{f-1} - y'u_{f-1})$, que l'on compare à $q(V) = q(u_f) = q(v_{f-1} - xu_{f-1})$. Or x est choisi pour que le résultat u_f approche au mieux la projection orthogonale de v_{f-1} sur $\langle u_{f-1} \rangle^\perp$. Toute autre combinaison linéaire entière de v_{f-1} et u_{f-1} aura donc une norme plus grande (preuve : écrivons $v^\perp = v - \tilde{x}u$ et $v_f = v - xu = v^\perp + (x - \tilde{x})u$ et un $v' = v - x'u = v^\perp + (x' - \tilde{x})u$. On a bien le résultat puisque $(x - \tilde{x}) \leq (x' - \tilde{x})$ pour tout entier x'.).

(3) On a $q(U + V) \geq q(V)$ équivaut à $q(U) + q(V) + 2(U, V) \geq q(V)$ d'où $(U, V) \geq -q(U)/2$. De même pour l'autre inégalité.

(4) Développons : $x_1^2 q(U) + x_2^2 q(V) + 2x_1 x_2 (U, V) < q(U)$. Or $|(U, V)| \leq q(U)/2$ donc
$$x_1^2 q(U) + x_2^2 q(V) - |x_1 x_2| q(U) < q(U)$$
soit encore
$$(x_1^2 - |x_1 x_2| - 1) q(U) + x_2^2 q(V) < 0.$$
Comme $q(V) \geq q(U)$, on a $x_1^2 + x_2^2 - |x_1 x_2| - 1 < 0$. Or $2|x_1 x_2| \leq x_1^2 + x_2^2$ donc l'inégalité précédente devient $|x_1 x_2| - 1 < 0$ ce qui implique $x_1 x_2 = 0$. Si $x_1 = 0$ mais pas x_2, on a $|x_2| q(V) \geq q(V) \geq q(U)$ donc l'inégalité du début est impossible, de même avec $x_2 = 0$ mais pas x_1.

(5) En raisonnant comme ci-dessus on a
$$(x_1^2 - |x_1 x_2|) q(U) + (x_2^2 - 1) q(V) < 0.$$
On a par hypothèse $x_2^2 - 1 \geq 0$ donc $x_1^2 + x_2^2 - |x_1 x_2| - 1 < 0$ et on termine la preuve comme ci-dessus.

(6) En effet, on a échangé u et v et à l'étape précédente on avait $q(u) < q(v)$.

(7) Si on n'est pas à la fin ou au début de l'algorithme alors $u = r = v' - xu' = v' \pm u'$ a une norme strictement plus petite que celle de $v = u'$, i.e. $q(v' \pm u') < q(u')$, soit à l'étape précédente
$$q(u'' \pm (v'' - x''u'')) < q(v'' - x''u'').$$
Autrement dit à cette étape, on aurait pu raccourcir v'' par un meilleur choix de x'', ce qui est impossible comme on l'a vu.

(8) Évident.

(9) Il suffit de développer $v = v^\perp + (u, v)/q(u)u$.

(10) On écrit $r = v^\perp + (u, r)/q(u)u = v^\perp + u((u, v) - x(u, u))/q(u)$. Donc
$$q(r) = q(v^\perp) + ((u, v) - q(u)x)^2 q(u) \leq q(v^\perp) + 1/4 q(u)$$
en utilisant la définition de x.

(11) On a que

$$q(v) \geq q(v^{\perp} + 9/4q(u) \geq q(r) - 1/4q(u) + 9/4q(u).$$

Si on n'est pas à la dernière itération $q(r) < q(u)$.

(12) On a $q(u)q(v) \geq 3q(r)q(u)$. Or à l'étape suivante $r = u'$ et $u = v'$. On a donc une décroissance d'un facteur 3 du produit. On a $1/3^{r-2}q(u_0)q(v_0) \geq \lambda_1^4$ où r est le nombre d'itération avec $|x| > 1$ d'où le résultat.

(13) On a $|(u, v)| \leq \sqrt{q(u)q(v)} < q(v) \leq q(v_0)$, donc un coût de $O(\log(q(v_0)))$ pour la boucle interne et un coût total de $O(\log(q(v_0))^3)$. En fait une analyse plus précise en coût amorti donne $O(\log(q(v_0))^2)$.