Correction of selected lattice exercises

1. Filtered Basis.

Let L be a d-rank lattice. Let $\vec{c}_1, \dots, \vec{c}_d \in L$ be linearly independent. For all $1 \leq i \leq d$, let $L_i = \text{span}(\vec{c}_1, \dots, \vec{c}_i) \cap L$.

---

1. *Show that for all $i \in \{1, \dots, d\}$, L_i is a lattice and that its rank is equal to i.*
2. *Let $2 \leq i \leq d$. Show that if $(\vec{b}_1, \dots, \vec{b}_{i-1})$ is a basis of L_{i-1}, there exists $\vec{b}_i \in L_i$ such that $\vec{b}_i \notin L_{i-1}$ and $(\vec{b}_1, \dots, \vec{b}_i)$ is a basis of L_i.*
3. *Deduce the existence of a basis $(\vec{b}_1, \dots, \vec{b}_d)$ of L such that $\text{span}(\vec{b}_1, \dots, \vec{b}_i) = \text{span}(\vec{c}_1, \dots, \vec{c}_i)$ for all $1 \leq i \leq d$.*

Cet exercice montre qu'on peut transformer une famille libre d'un réseau en une base, en conservant les sous-espaces engendrés. Il montre en particulier que tout réseau admet une base, de façon duale à la démonstration vue en cours, qui était :

— On prend un vecteur primitif du réseau $\vec{b}_1$, comme un plus court vecteur du réseau.
— Soit π la projection orthogonale sur $\vec{b}^{\perp}$. Si $(\pi(\vec{b}_2), \dots, \pi(\vec{b}_d))$ est une base de $\pi(L)$, alors $(\vec{b}_1, \dots, \vec{b}_d)$ est une base de L.

---

1. *Comme L_i est l'intersection d'un réseau avec un espace vectoriel, c'est un réseau. En outre, L_i est inclus dans l'espace $(\vec{c}_1, \dots, \vec{c}_i)$ qui est de dimension i, donc le rang de L_i est $\leq i$. Mais comme $\vec{c}_1, \dots, \vec{c}_i \in L_i$, le rang est aussi $\geq i$, donc il y a en fait égalité.*
2. *Soit π la projection orthogonale sur $(\vec{b}_1, \dots, \vec{b}_{i-1})^{\perp}$. On montre facilement que $\pi(L_i)$ est un réseau de dimension 1. Et si $\pi(\vec{b}_i)$ une base de $\pi(L_i)$, alors $\vec{b}_i \in L_i \setminus L_{i-1}$ et on montre que $(\vec{b}_1, \dots, \vec{b}_{i-1}, \vec{b}_i)$ est une base de L_i. Plusieurs personnes ont écrit qu'on pouvait prendre $\vec{b}_i \in L_i \setminus L_{i-1}$ de norme minimale, ou engendreant $(\vec{c}_i) \cap L_i$: c'est faux, car $(\vec{b}_1, \dots, \vec{b}_{i-1}, \vec{b}_i)$ n'est alors pas nécessairement une base de L_i. Pour s'en convaincre, prenons le réseau L formé par tous les quadruplets $(x_1, \dots, x_4) \in \mathbb{Z}^4$ tels que $x_1 + \dots + x_4$ soit pair. Et prenons $\vec{c}_1 = (1, 1, 0, 0)$, $\vec{c}_2 = (1, -1, 0, 0)$, $\vec{c}_3 = (0, 0, 1, 1)$ et $\vec{c}_4 = (0, 0, 1, -1)$. On a vu en cours que $(\vec{c}_1, \dots, \vec{c}_4)$ n'était pas une base de L, alors que les $\vec{c}_i$ sont orthogonaux deux à deux. Dans les mauvaises constructions, il est possible de prendre $(\vec{b}_1, \dots, \vec{b}_4) = (\vec{c}_1, \dots, \vec{c}_4)$.*
3. *Il suffit d'itérer la question précédente, en commençant par une base $\vec{b}_1$ de L_1.*

---

2. Computing a Basis.

For any vectors $\vec{b}_1, \dots, \vec{b}_m \in \mathbb{R}^n$, we let :

$$L(\vec{b}_1, \dots, \vec{b}_m) = \left\{ \sum_{i=1}^{m} x_i \vec{b}_i, x_i \in \mathbb{Z} \right\}.$$

For $1 \leq i \leq m$, let $\vec{b}_i^\star$ be the orthogonal projection of $\vec{b}_i$ over $\mathrm{span}(\vec{b}_1, \ldots, \vec{b}_{i-1})^\perp$: in particular, $\vec{b}_1^\star = \vec{b}_1$. We define for $1 \leq j < i \leq m$: $\mu_{i,j} = \frac{\langle \vec{b}_i, \vec{b}_j^\star \rangle}{\|\vec{b}_j^\star\|^2}$ if $\vec{b}_j^\star \neq 0$, and 0 otherwise. Then, for each $1 \leq i \leq m$:

$$\vec{b}_i = \vec{b}_i^\star + \sum_{j=1}^{i-1} \mu_{i,j} \vec{b}_j^\star.$$

We recall that if the $\vec{b}_i$'s are in $\mathbb{Z}^n$:

— all $\mu_{i,j} \in \mathbb{Q}$ and can be computed in time polynomial in M, n and m, where $M = \log(1 + \max_{i=1}^m \|\vec{b}_i\|)$.

— Given any $1 \leq i \leq n$, the size-reduction algorithm can modify $\vec{b}_i$ in polynomial time without changing $L(\vec{b}_1, \ldots, \vec{b}_m)$ in such a way that $|\mu_{i,j}| \leq 1/2$ for all $j < i$, .

---

1. *Assume first that $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{Z}^n$ such that $\vec{b}_m^\star = 0$ and $\vec{b}_i^\star \neq 0$ for all $1 \leq i \leq m-1$. Let π be the orthogonal projection over $\mathrm{span}(\vec{b}_1, \ldots, \vec{b}_{m-2})^\perp$. Show that $\pi(\vec{b}_{m-1}) = \vec{b}_{m-1}^\star$ and $\pi(\vec{b}_m) = \mu_{m,m-1}\vec{b}_{m-1}^\star$.*
2. *Next, write $\mu_{m,m-1} = \frac{p}{q}$ as an irreducible fraction. Given (p, q), Euclid's extended algorithm computes $(u, v) \in \mathbb{Z}^2$ in polynomial time such that $up + vq = 1$. Show that if we replace $(\vec{b}_{m-1}, \vec{b}_m)$ by $(p\vec{b}_{m-1} - q\vec{b}_m, v\vec{b}_{m-1} + u\vec{b}_m)$, then $L(\vec{b}_1, \ldots, \vec{b}_m)$ does not change and the new Gram-Schmidt vectors satisfy : $\vec{b}_{m-1}^\star = 0$ and $\vec{b}_m^\star \neq 0$.*
3. *Deduce a polynomial-time algorithm which, given $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{Z}^n$ such that $\vec{b}_m^\star = 0$ and $\vec{b}_i^\star \neq 0$ for all $1 \leq i \leq m-1$, outputs a basis of the lattice $L(\vec{b}_1, \ldots, \vec{b}_m)$. Hint : Use size-reduction and make sure that $\max_{i=1}^m \|\vec{b}_i^\star\|$ never increases during the execution of the algorithm.*
4. *Deduce a polynomial-time algorithm which, given $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{Z}^n$, outputs a basis of the lattice $L(\vec{b}_1, \ldots, \vec{b}_m)$.*

Cet exercice montre comment généraliser l'algorithme d'Euclide de calcul du pgcd au problème de calculer une base d'un réseau $L(\vec{b}_1, \ldots, \vec{b}_m)$.

1. *Il suffit d'utiliser la décomposition* $\vec{b}_i = \vec{b}_i^\star + \sum_{j=1}^{i-1} \mu_{i,j}\vec{b}_j^\star$, *et la linéarité de la projection.*

2. *La transformation qui envoie* $(\vec{b}_{m-1}, \vec{b}_m)$ *vers* $(p\vec{b}_{m-1} - q\vec{b}_m, v\vec{b}_{m-1} + u\vec{b}_m)$ *est linéaire de déterminant* $up + vq = 1$, *donc elle laisse invariante le réseau* $L(\vec{b}_{m-1}, \vec{b}_m)$. *En utilisant la question précédente et la linéarité de la projection, on obtient que le nouveau vecteur satisfait* $\vec{b}_{m-1}^\star = 0$. *Et* $\vec{b}_m^\star \neq 0$ *car* $(\vec{b}_1, \ldots, \vec{b}_m)$ *est inchangé. De plus, on remarque que* $\max(\|\vec{b}_{m-1}^\star\|, \|\vec{b}_m^\star\|)$ *diminue. En effet, avant transformation, le réseau* $L(\pi(\vec{b}_{m-1}), \pi(\vec{b}_m))$ *n'est autre que* $\frac{\vec{b}_{m-1}^\star}{q}\mathbb{Z}$ *d'après la première question. Après transformation,* $\pi(\vec{b}_m) = \frac{\vec{b}_{m-1}^\star}{q}$, *donc la nouvelle norme* $\|\vec{b}_m^\star\|$ *est inférieure ou égale à l'ancienne* $\|\vec{b}_{m-1}^\star\|$ *car* $1/|q| \leq 1$. *Certains ont écrit une égalité, mais ce n'est pas vrai : pour s'en convaincre, il suffit de simuler l'algorithme d'Euclide du pgcd en prenant* $\vec{b}_1 = (a)$ *et* $\vec{b}_2 = (b)$.

3. *On a envie d'itérer la question précédente jusqu'à ce que* $\vec{b}_1^\star = 0$, *c'est-à-dire* $\vec{b}_1 = 0$, *mais il faut garantir que les vecteurs restent polynomiaux en la taille initiale : chaque transformation* $(p\vec{b}_{m-1} - q\vec{b}_m, v\vec{b}_{m-1} + u\vec{b}_m)$ *risque d'augmenter la norme des* $\vec{b}_i$, *seul son coût local est polynomial. Considérons l'algorithme 1. On sait que* $L(\vec{b}_1, \ldots, \vec{b}_m)$ *ne change jamais d'après la question précédente. Or à la fin de la boucle, on sait que* $\vec{b}_1 = 0$ *et que tous les* $\vec{b}_i^\star$ *sont* $\neq 0$ *pour* $i \geq 2$, *donc* $(\vec{b}_2, \ldots, \vec{b}_m)$ *est une base de* $L(\vec{b}_1, \ldots, \vec{b}_m)$ *: l'algorithme est correct. Appelons* $M_j = \max_{1\leq k\leq m} \|\vec{b}_k^\star\|$ *à la* j*-ième itération de boucle : Comme la size-reduction ne change pas les vecteurs de Gram-Schmidt, on a démontré dans la question précédente que* $M_{j+1} \leq M_j \leq \ldots M_0$. *Après la size-reduction, on a par définition :* $\|\vec{b}_k\| \leq mM_j \leq mM_0 \leq$ *pour tout* $1 \leq k \leq m$. *On en déduit que durant toute la boucle FOR, les vecteurs ont une taille polynomiale en* m *et* $\log M_0$. *Or toutes les autres opérations sont polynomiales en la taille des vecteurs. On a donc montré que l'algorithme était polynomial.*

4. *On en déduit l'algorithme 2. Chaque appel de l'algorithme 1 a un coût polynomial en la taille courante, mais il faut s'assurer que la taille courante est polynomiale en la taille initiale. Pour cela, on utilise à nouveau le fait que* $\max_{1\leq k\leq m} \|\vec{b}_k^\star\|$ *n'augmente jamais, et donc que* $\max_{1\leq k\leq m} \|\vec{b}_k\|$ *reste polynomial en la taille initiale.*

Algorithm 1 Premier algorithme

Input: $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{Z}^n$ tels que $\vec{b}_m^\star = 0$ et $\vec{b}_i^\star \neq 0$ pour tout $1 \leq i \leq m-1$,
Output: une base du réseau $L(\vec{b}_1, \ldots, \vec{b}_m)$.

1: **for** $i = m$ à 2 **do**
2: Calculer la décomposition de Gram-Schmidt de $(\vec{b}_1, \ldots, \vec{b}_m)$
3: Remplacer $(\vec{b}_{i-1}, \vec{b}_i)$ by $(p\vec{b}_{i-1} - q\vec{b}_i, v\vec{b}_{i-1} + u\vec{b}_i)$ où $\mu_{i,i-1} = \frac{p}{q}$ comme fraction irréductible.
4: Réduire $\vec{b}_{i-1}$ et $\vec{b}_i$ par *size-reduction*.
5: **end for**
6: Renvoyer $(\vec{b}_2, \ldots, \vec{b}_m)$

Algorithm 2 Deuxième algorithme

Input: $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{Z}^n$
Output: une base du réseau $L(\vec{b}_1, \ldots, \vec{b}_m)$.

1: **for** $i = 1$ à m **do**
2: Calculer la décomposition de Gram-Schmidt de $(\vec{b}_1, \ldots, \vec{b}_i)$
3: **if** $\vec{b}_i^\star = 0$ **then**
4: Remplacer $(\vec{b}_1, \ldots, \vec{b}_i)$ par les vecteurs renvoyés par l'algorithme 1 avec comme entrée $(\vec{b}_1, \ldots, \vec{b}_i)$
5: **end if**
6: **end for**
7: Renvoyer $(\vec{b}_1, \ldots, \vec{b}_m)$: il y a potentiellement moins de m vecteurs car chaque étape 4 enlève un vecteur.

3. Lagrange's Algorithm.

In 1773, Lagrange published a two-dimensional reduction algorithm (Algorithm 3) which is an ancestor of the LLL algorithm.

Algorithm 3 Lagrange's reduction algorithm.

Input: a basis $(\vec{u}, \vec{v})$ of a two-rank lattice L.
Output: a Lagrange-reduced basis of L.

1: **if** $\|\vec{u}\| < \|\vec{v}\|$ **then**
2: swap $\vec{u}$ and $\vec{v}$
3: **end if**
4: **repeat**
5: $\vec{r} \longleftarrow \vec{u} - q\vec{v}$ where $q = \left\lfloor \frac{\langle \vec{u}, \vec{v} \rangle}{\|\vec{v}\|^2} \right\rceil$ and $\lfloor x \rceil$ denotes an integer closest to x.
6: $\vec{u} \longleftarrow \vec{v}$
7: $\vec{v} \longleftarrow \vec{r}$
8: **until** $\|\vec{u}\| \leq \|\vec{v}\|$
9: Output $(\vec{u}, \vec{v})$.

1. *Consider Line 5 of Algorithm 3 : show that this choice of $q \in \mathbb{Z}$ minimizes $\|\vec{u} - q\vec{v}\|$.*
2. *Show that Lagrange's algorithm terminates,* i.e. *that the repeat/until loop is not infinite.*
3. *Consider the integer q of Step 5. Show that :*
   — *if $q = 0$, then this must be the last iteration of the loop.*
   — *if $|q| = 1$, then this must be either the first or last iteration of the loop.*
4. *Show that the number τ of iterations of the repeat/until loop is bounded by : $\tau = O(1 + \log B - \log \lambda_1(L))$ where B denotes the maximal Euclidean norm of the input basis vectors $\vec{u}$ and $\vec{v}$.*
5. *Show that when $L \subseteq \mathbb{Z}^n$, the bit-complexity of Lagrange's algorithm is polynomial in $\log B$.*

Cet algorithme ressemble beaucoup à l'algorithme d'Euclide, mais son analyse diffère un peu. Pour plus d'informations sur l'algorithme de Lagrange et sa géneralisation en dimension supérieure, voir `https://perso.ens-lyon.fr/damien.stehle/downloads/lowdim-final.pdf` .

1. *On a :* $\|\vec{u} - q\vec{v}\|^2 = \|\vec{u}\|^2 - 2q\langle\vec{u},\vec{v}\rangle + q^2\|\vec{v}\|^2$. *Son minimum sur* $\mathbb{R}$ *est donc atteint en* $q_0 = \frac{\langle\vec{u},\vec{v}\rangle}{\|\vec{v}\|^2}$. *Or* $q = q_0$ *est un axe de symétrie de cette parabole, donc le minimum sur* $\mathbb{Z}$ *est atteint en* $\lfloor q_0 \rceil$. *Cette question montre que l'algorithme de Lagrange est glouton. Attention, contrairement à ce que plusieurs personnes ont sous-entendu : si une fonction* f *admet un minimum sur* $\mathbb{R}$ *en* x_0, *son minimum sur* $\mathbb{Z}$ *n'est pas nécessairement en* $\lfloor x_0 \rceil$. *Ici, c'est vrai parce que* f *est une fonction polynomiale du second degré.*

2. *On remarque tout d'abord un invariant de boucle :* $(\vec{u},\vec{v})$ *est une base de* L. *Si la boucle de l'étape 8 ne s'arrête pas, c'est que* $\|\vec{u}\| > \|\vec{v}\|$, *et il existe alors une suite de vecteurs du réseau dont la norme est strictement décroissante et non nulle car chaque* $(\vec{u},\vec{v})$ *est une base de* L. *Or on a vu en cours que l'intersection d'un réseau avec une boule est finie : contradiction.*

3. — *Si* $q = 0$, *les étapes 5 à 8 ne font qu'échanger* $\vec{u}$ *et* $\vec{v}$. *Or on remarque qu'au début de chaque itération de boucle, on a* $\|\vec{u}\| \geq \|\vec{v}\|$. *En effet, c'est vrai pour la première itération de boucle à cause des trois premières lignes. Et c'est vrai aussi pour les autres itérations à cause de la condition de sortie à la ligne 8. Donc, après échange, on a forcément* $\|\vec{u}\| \leq \|\vec{v}\|$, *donc la boucle s'arrête : c'est bien la dernière itération.*
   — *Si* $|q| = 1$ *et que ce n'est pas la dernière itération, on a* $\|\vec{u}\hat{A} + q\vec{v}\| < \|\vec{v}\|$. *Comme* $q = \pm 1$, *on en déduit que* $\min_{q'\in\mathbb{Z}} \|q'\vec{u}\hat{A} + \vec{v}\| < \|\vec{v}\|$, *ce qui ne peut arriver qu'à la première itération, car l'algorithme est glouton : pour toute itération qui n'est pas la première,* $\vec{v}$ *ne peut être raccourci en lui soustrayant un multiple de* $\vec{u}$.

4. *On en déduit que pour toute itération qui n'est ni la première, ni la dernière, on a* $|q| \geq 2$. *Donc* $|\mu| \geq \frac{3}{2}$ *où* $\mu = \frac{\langle\vec{u},\vec{v}\rangle}{\|\vec{v}\|^2}$. *Or* $\vec{u} = \mu\vec{v} + \vec{w}$ *avec* $\vec{w}$ *la projection orthogonale de* $\vec{u}$ *sur l'hyperplan* $\vec{v}^\perp$. *Donc* $\|\vec{u}\|^2 = \mu^2\|\vec{v}\|^2 + \|\vec{w}\|^2 \geq \frac{9}{4}\|\vec{v}\|^2 + \|\vec{w}\|^2$. *Donc* $\|\vec{v}\|^2 \leq \frac{4}{9}\hat{A}\ \|\vec{u}\|^2$. *Mais comme ce* $\vec{v}$ *n'est autre que le prochain* $\vec{u}$, *on en déduit qu'à chaque itération, sauf éventuellement les deux premières et la dernière,* $\|\vec{u}\|^2$ *va diminuer d'un facteur mutiplicatif* $\geq \frac{9}{4}$. *On conclut puisque* $\|\vec{u}\| \geq \lambda_1(L)$ *car* $\vec{u} \neq 0$ *puisque* $(\vec{u},\vec{v})$ *est toujours une base.*

5. *Soit* $M = \max(\|\vec{u}\|, \|\vec{v}\|)$ *au début de l'algorithme de Lagrange. On remarque l'invariant de boucle :* $\|\vec{u}\| \leq M$ *et* $\|\vec{v}\| \leq M$, *donc chaque opération de l'algorithme est polynomiale en* $\log M$. *Or il y a un nombre polynomial d'itérations de boucle, donc l'algorithme de Lagrange est polynomial. Une analyse plus précise montre qu'on peut implémenter l'algorithme de Lagrange en temps quadratique, en utilisant l'algorithme de division euclidienne usuel, sans utiliser de transformée de Fourier.*