Lattice Exercises

Notation :

- $\langle \vec{u}, \vec{v} \rangle$ is the standard Euclidean inner product of $\mathbb{R}^n$, that is $\langle \vec{u}, \vec{v} \rangle = \sum_{i=1}^n u_i v_i$.
- The Euclidean norm : $\|\vec{u}\|^2 = \langle \vec{u}, \vec{u} \rangle$.
- span() denotes the subspace generated by the vectors or the set inside the parentheses. It is the smallest subspace containing the vectors or the set inside the parentheses.
- $\mathcal{B}_r(\vec{v}) = \{\vec{w} \in \mathbb{R}^n, \|\vec{v} - \vec{w}\| < r\}$ is the open ball of $\mathbb{R}^n$ of center $\vec{v}$ and radius r.

1. Gram-Schmidt Orthogonalization. $(\star)$

Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{R}^m$. For $1 \leq i \leq n$, 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, $\vec{b}_1^\star = \vec{b}_1$. Show that :

---

1. *The Gram-Schmidt vectors $\vec{b}_i^\star$'s are pairwise orthogonal.*
2. $\mathrm{vol}(\vec{b}_1, \ldots, \vec{b}_n) = \prod_{i=1}^n \|\vec{b}_i^\star\|$.
3. *The vectors $\vec{b}_1, \ldots, \vec{b}_n$ are linearly independent iff the Gram-Schmidt vectors $\vec{b}_i^\star$'s are all non zero.*
4. *For any $1 \leq i \leq n$, there exist $\mu_{i,1}, \ldots, \mu_{i,i-1}$ such that $\vec{b}_i = \vec{b}_i^\star + \sum_{j=1}^{i-1} \mu_{i,j} \vec{b}_j^\star$. If $\vec{b}_1, \ldots, \vec{b}_n$ are linearly independent, then the $\mu_{i,j}$'s are unique.*

---

2. Filtered Basis. $(\star\star)$

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

---

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

---

3. Short Bases. $(\star\star)$

Let L be a d-rank lattice. Let $\vec{c}_1, \ldots, \vec{c}_d \in L$ be linearly independent. Show that :

---

1. *There exists a basis $B = (\vec{b}_1, \ldots, \vec{b}_d)$ of L such that $\|\vec{b}_i^\star\| \leq \|\vec{c}_i^\star\|$ and $\mathrm{span}(\vec{b}_1, \ldots, \vec{b}_i) = \mathrm{span}(\vec{c}_1, \ldots, \vec{c}_i)$ for $1 \leq i \leq d$.*
2. *One can further satisfy : $\|\vec{b}_i\|^2 \leq \|\vec{b}_i^\star\|^2 + \sum_{j=1}^{i-1} \|\vec{b}_j^\star\|^2/4$.*

---

4. Integral Gram-Schmidt. $(\star\star)$

Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Z}^m$ be linearly independent. Let the $\vec{b}_i^\star$ be its Gram-Schmidt vectors. Show that :

---

1. *For* $1 \leq j < i$, $\mu_{i,j} = \langle \vec{b}_i, \vec{b}_j^\star \rangle / \|\vec{b}_j^\star\|^2 \in \mathbb{Q}$.
2. $\|\vec{b}_i^\star\|^2 = \|\vec{b}_i\|^2 - \sum_{j=1}^{i-1} \mu_{i,j}^2 \|\vec{b}_j^\star\|^2$ *for* $1 \leq i \leq n$.
3. *For* $1 \leq j < i$, $\mu_{i,j} = \frac{\langle \vec{b}_i, \vec{b}_j \rangle - \sum_{k=1}^{j-1} \mu_{j,k}\mu_{i,k}\|\vec{b}_k^\star\|^2}{\|\vec{b}_j^\star\|^2}$.
4. *If* $d_0 = 1$ *and* $d_k = \det_{1 \leq i,j \leq k} \langle \vec{b}_i, \vec{b}_j \rangle$ *for* $1 \leq k \leq n$, *then* $d_{k-1}\vec{b}_k^\star \in L(\vec{b}_1, \ldots, \vec{b}_k)$ *for* $1 \leq k \leq n$ *and* $\lambda_{i,j} = d_j \mu_{i,j} \in \mathbb{Z}$ *for* $1 \leq j < i$.
5. *One can compute all the integers* d_k*'s and* $\lambda_{i,j}$*'s in polynomial time.*

---

5. Kernel Lattices. ($\star$)

Let A be an $m \times n$ matrix over $\mathbb{Z}$. Let L_A be the set of $\vec{x} \in \mathbb{Z}^m$ such that $\vec{x}A \equiv 0 \pmod q$. Show that :

---

1. L_A *is a full-rank lattice in* $\mathbb{Z}^m$.
2. $\mathrm{vol}(L_A)$ *is an integer dividing* q^n.
3. *The dual lattice of* L_A *is* $(1/q)\Lambda_A$ *where* Λ_A *is the set of* $\vec{y} \in \mathbb{Z}^m$ *such that* $\vec{y}\hat{A} \equiv \vec{z}A^t \pmod q$ *for some* $\vec{z} \in \mathbb{Z}^n$, *where* A^t *denotes the transpose of* A.

---

6. SIS and LWE Lattices. ($\star$)

Let G be a finite Abelian group : we view G as $\mathbb{Z}$-module, so that the notation ng for $(n, g) \in \mathbb{Z} \times G$ is defined. Let $g_1, \ldots, g_m \in G$. Show that :

---

1. *The set* L *of* $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ *such that* $\sum_{i=1}^m x_i g_i = 0$ *in* G *is a lattice in* $\mathbb{Z}^m$.
2. *The rank of* L *is* m.
3. *The volume of* L *divides the order of* G.
4. *The dual lattice of* L *is the lattice* Λ *defined as the set of all* $(y_1, \ldots, y_m) \in \mathbb{R}^m$ *such that there exists a morphism* $s : G \to \mathbb{R}/\mathbb{Z}$ *satisfying* $s(g_i) = y_i$ *mod 1 for all* $1 \leq i \leq m$. *Such a map* s *is called an* additive character *of* G.
5. *The set of additive characters of* G *is an additive group, isomorphic to* G.

---

7. Computing a Basis. ($\star\star$)

For any vectors $\vec{b}_1, \ldots, \vec{b}_m \in \mathbb{R}^n$, we let : $L(\vec{b}_1, \ldots, \vec{b}_m) = \left\{ \sum_{i=1}^m x_i \vec{b}_i, x_i \in \mathbb{Z} \right\}$. 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* $L(\vec{b}_1, \ldots, \vec{b}_m)$.