Gram-Schmidt Orthogonalization

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.

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 $\text{span}(\vec{b}_1, \ldots, \vec{b}_{i-1})^\perp$: $\vec{b}_i^\star$ is orthogonal to $\text{span}(\vec{b}_1, \ldots, \vec{b}_{i-1})$, and $\vec{b}_i - \vec{b}_i^\star$ belongs to $\text{span}(\vec{b}_1, \ldots, \vec{b}_{i-1})$. 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. *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.*
3. *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 $\vec{b}_j^\star \neq 0$, then $\mu_{i,j} = \langle \vec{b}_i, \vec{b}_j^\star \rangle / \|\vec{b}_j^\star\|^2$.*
4. $\text{vol}(\vec{b}_1, \ldots, \vec{b}_n) = \prod_{i=1}^{n} \|\vec{b}_i^\star\|$.

---

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

Let $\vec{b}_1, \ldots, \vec{b}_n \in \mathbb{Z}^m$ be linearly independent. Let the $\vec{b}_i^\star$'s 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.*

---

3. The Gram-Schmidt Lattice. ($\star\star$)

Let $B = (\vec{b}_1, \ldots, \vec{b}_n)$ be a basis of a lattice $L \subseteq \mathbb{R}^m$. Let L_B be the lattice generated by its Gram-Schmidt vectors $\vec{b}_i^\star$.

---

1. *Show that* $\text{vol}(L_B) = \text{vol}(L)$.
2. *Show that* $\lambda_1(L_B) = \min_i \|\vec{b}_i^\star\|$.
3. *Show that* $\lambda_1(L) \geq \lambda_1(L_B)$.
4. *Let $\mu(L)$ denote the covering radius of L : this is the maximal distance between L and a point of* $\text{span}(L)$. *What is $\mu(L_B)$? Show that $\mu(L) \leq \mu(L_B)$.*
