Lecture 3

Lattice Problems and Rounding Algorithms - Part II

1 Orthogonal Projections

DEFINITION 1 *The Gram-Schmidt Orthogonalization (GSO)* $\mathbf{B}^\star$ *of a non-singular matrix* $\mathbf{B}$ *is defined by* $\mathbf{b}_i^\star = \pi_i(\mathbf{b}_i)$ *where* π_i *denotes the projection orthogonal to the span of* $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$.

The projections π_i can be given explicitly by recursion:

$$\pi_i : \mathbf{x} \mapsto \mathbf{x} - \sum_{j<i} \frac{\langle \mathbf{x}, \mathbf{b}_j^\star \rangle}{\|\mathbf{b}_j^\star\|_2^2} \mathbf{b}_j^\star.$$

We recall some key properties of the Gram-Schmidt Orthogonalization:

- $\mathbf{b}_1^\star = \mathbf{b}_1$
- $\mathrm{Span}_\mathbb{R}(\mathbf{b}_1, \ldots, \mathbf{b}_j) = \mathrm{Span}_\mathbb{R}(\mathbf{b}_1^\star, \ldots, \mathbf{b}_j^\star)$ for all $j \leq n$
- $\mathbf{b}_i^\star \perp \mathbf{b}_j^\star$ for all $i \neq j$
- $\mathbf{b}_i \perp \mathbf{b}_j^\star$ for all $i < j$.

The Gram-Schmidt Orthogonalization can also be written as a matrix decomposition: $\mathbf{B} = \mathbf{B}^\star \cdot \mathbf{T}$ where $\mathbf{T}$ is an upper triangular matrix with unit diagonal and $\mathbf{B}^\star$ has orthogonal row. In particular $\det(\mathbf{T}) = 1$, and therefore if $\mathbf{B}$ is a basis of a lattice L we have

$$\prod_{i=1}^n \|\mathbf{b}_i^\star\|_2 = \sqrt{|\det(\mathbf{B}^{\star\top} \mathbf{B}^\star)|} = \sqrt{|\det(\mathbf{B}^\top \mathbf{B})|} = \det(L).$$

Note however that $\mathbf{T}$ is not necessarily integral: $\mathbf{B}^\star$ is not necessarily a basis of L! And yet, we will see that $\mathcal{P}(\mathbf{B}^\star)$ is also a tiling of L.

For any non-zero vector $\mathbf{v}$, we denote by $\pi_\mathbf{v}^\perp : \mathbf{x} \mapsto \mathbf{x} - \frac{\langle \mathbf{x}, \mathbf{v} \rangle}{\|\mathbf{v}\|_2^2} \mathbf{v}$ the projection orthogonally to $\mathbf{v}$.

THEOREM 2 *Let* L *be a rank* k *lattice, and* $\mathbf{v} \in L$. *Then,* $\pi_\mathbf{v}^\perp(L)$ *is a lattice of rank* $k-1$.

PROOF: Because $\pi_\mathbf{v}^\perp$ is linear, $L' = \pi_\mathbf{v}^\perp(L)$ is a group. To prove that it is discrete, we claim that any $\mathbf{x} \in \pi_\mathbf{v}^\perp(L)$ has a pre-image $\mathbf{y} \in L$ such that $|\langle \mathbf{y}, \mathbf{v} \rangle| \leq \frac{1}{2}\|\mathbf{v}\|^2$; i.e. there exists a pre-image of $\mathbf{x}$ in $\mathbf{x} + [-1/2, 1/2) \cdot \mathbf{v}$. Indeed, consider an arbitrary pre-image $\mathbf{y}'$ of $\mathbf{x}$, and set $k = \left\lfloor \frac{\langle \mathbf{y}', \mathbf{v} \rangle}{\|\mathbf{v}\|^2} \right\rceil \in \mathbb{Z}$, and set $\mathbf{y} = \mathbf{y}' - k\mathbf{v}$.

If L' were not discrete, it would contain infinitely many distinct points in the unit ball $\mathfrak{B}$. Each of them can be lifted to a distinct point of L in the body $\mathfrak{B} + [-1/2, 1/2] \cdot \mathbf{v}$, which is a bounded: this would imply that L is not discrete.

Regarding the rank, we note the inclusion $\mathrm{Span}_\mathbb{R}(L') \subset \pi_\mathbf{v}^\perp(\mathrm{Span}_\mathbb{R}(L))$. Since $\mathbf{v} \in \mathrm{Span}_\mathbb{R}(L)$, the dimension of $\pi_\mathbf{v}^\perp(\mathrm{Span}_\mathbb{R}(L))$ is $k-1$, so the rank of L' is at most $k-1$. We also note that $\mathrm{Span}_\mathbb{R}(L') + \mathbf{v} \cdot \mathbb{R} \supseteq \mathrm{Span}_\mathbb{R}(L)$, hence the rank of L' is at least $k-1$. □

The process by which we chose a particular lift $\mathbf{y}$ of $\mathbf{x}$ in the segment $\mathbf{x} + [-1/2, 1/2) \cdot \mathbf{v}$ will be central in many algorithms to follow, referred to as the **nearest plane method** or as **size-reduction**. Note that in general, such a lift may not be unique. This can happen if $\mathbf{v}$ is not *primitive* with respect to L, that is if $\mathbf{v}$ is an integral multiple of another vector $\mathbf{v} = j \cdot \mathbf{w}$ for some integer $j > 1$. This is in fact, the only exception to uniqueness.

Definition 3 (Primitive Vector) *A non-zero vector* $\mathbf{v}$ *in a lattice* L *is said primitive (with respect to* L*) if* $(\mathbf{v} \cdot \mathbb{R}) \cap L = \mathbf{v} \cdot \mathbb{Z}$. *Equivalently, it is primitive if* $\frac{1}{j}\mathbf{v} \notin L$ *for any integer* $j > 1$.

Lemma 4 *A vector* $\mathbf{v}$ *in a lattice* L *is primitive if and only if* $\mathbf{v}$ *is part of some basis of* L.

Proof: Let $\mathbf{B}$ be a basis of L with $\mathbf{b}_1 = \mathbf{v}$. Let j be a positive integer such that $\mathbf{w} = \frac{1}{j}\mathbf{v}$ is in L. Because $\mathbf{w} \in L$, we can write $\mathbf{w} = \mathbf{B} \cdot \mathbf{x}$ for some non-zero integer vector $\mathbf{x} \in \mathbb{Z}^n$. It can also be written as $\mathbf{w} = \mathbf{B} \cdot (1/j, 0, \ldots, 0)$; because $\mathbf{B}$ is non singular this implies $\mathbf{x} = (1/j, 0, \ldots, 0)$, and therefore that $j = 1$.

Reciprocally, let $\mathbf{v}$ be primitive, and let $\mathbf{B}'$ be a basis of $L' = \pi_{\mathbf{v}}(L)$. Let $\mathbf{b}_i$ be a pre-image in L of $\mathbf{b}'_i$ for each $i \in \{1, \ldots, n-1\}$. We claim that setting $\mathbf{b}_n = \mathbf{v}$ makes $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ into a basis of L. By construction, all the $\mathbf{b}_i$ belong to L so $\mathbf{B}$ generates a sublattice S of L. Furthermore, S and L have the same rank, so any vector $\mathbf{w}$ of L writes as $\mathbf{B} \cdot \mathbf{x}$ for some *real* vector $\mathbf{x} \in \mathbb{R}^n$; we need to prove that $\mathbf{x}$ is in fact integer. Note that $\pi_{\mathbf{v}}(\mathbf{w}) = \sum_{i=1}^{n-1} x_i \mathbf{b}'_i$, and that it belongs to L', hence the x_i's are all integers for $i \in \{1 \ldots n-1\}$. Substracting $\sum_{i=1}^{n-1} x_i \mathbf{b}_i$ from $\mathbf{w}$, we get that $\mathbf{B} \cdot (0, 0, \ldots, 0, x_n)$ belongs to L, that is $x_n \cdot \mathbf{v} \in L$: by primitivity of $\mathbf{v}$, x_n is an integer. Hence $\mathbf{B}$ is indeed a basis of L. $\square$

2 The Nearest Plane Algorithm and the $\mathcal{P}(\mathbf{B}^\star)$ Tiling

Lemma 5 *Let* $\mathbf{v}$ *be a primitive vector of a lattice* L*, define* $L' = \pi^\perp_{\mathbf{v}}(L)$*, and let* T' *be a tiling of* L'*. Then* $T = T' + [-1/2, 1/2) \cdot \mathbf{v}$ *is a tiling of* L.

Proof: Let us shorten $\pi^\perp_{\mathbf{v}}$ as π. We start by showing that T is covering for L. Any target $\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(L)$ as $\mathbf{t} = t_1\mathbf{v} + \mathbf{t}'$ where $\mathbf{t}' = \pi(\mathbf{t}) \in \mathrm{Span}_{\mathbb{R}}(L')$. Because T' is covering for L', $\mathbf{t}'$ can be written as $\mathbf{t}' = \mathbf{e}' + \mathbf{w}'$ for some $\mathbf{e}' \in T'$ and $\mathbf{w}' \in L'$. Let $\mathbf{w}'' \in L$ be a pre-image of $\mathbf{w}'$ for π, in particular $\mathbf{w}'' = \mathbf{w}' + w_1\mathbf{v}$ for some $w_1 \in \mathbb{R}$. Unrolling, we have:

$$\begin{aligned}
\mathbf{t} &= t_1\mathbf{v} + \mathbf{t}' \\
&= t_1\mathbf{v} + \mathbf{e}' + \mathbf{w}' \\
&= (t_1 - w_1)\mathbf{v} + \mathbf{e}' + \mathbf{w}'' \\
&= \underbrace{((t_1 - w_1) - \lfloor t_1 - w_1 \rceil) \cdot \mathbf{v}}_{\in[-1/2,1/2)\cdot\mathbf{v}} + \underbrace{\mathbf{e}'}_{\in T'} + \underbrace{\lfloor t_1 - w_1 \rceil \cdot \mathbf{v} + \mathbf{w}''}_{\in L}
\end{aligned}$$

and we conclude that $T = T' + [-1/2, 1/2) \cdot \mathbf{v}$ is covering for L.

We now prove that T is packing for L. Let $\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(L)$ and let $\mathbf{e} + \mathbf{f} + \mathbf{w} = \mathbf{e}' + \mathbf{f}' + \mathbf{w}' = \mathbf{t}$ were $\mathbf{e}, \mathbf{e}' \in T'$, $\mathbf{f}, \mathbf{f}' \in [-1/2, 1/2) \cdot \mathbf{v}$ and $\mathbf{w}, \mathbf{w}' \in L$. Note that $\pi(\mathbf{t}) = \mathbf{e} + \pi(\mathbf{w}) = \mathbf{e}' + \pi(\mathbf{w}')$ where $\pi(\mathbf{w}), \pi(\mathbf{w}') \in L'$. Since T' is L' packing we have that $\mathbf{e} = \mathbf{e}'$ and that $\pi(\mathbf{w}) = \pi(\mathbf{w}')$. The kernel of π over L is $(\mathbb{R} \cdot \mathbf{v}) \cap L$, which by primitivity is exactly $\mathbf{v} \cdot \mathbf{Z}$, so $\mathbf{w} - \mathbf{w}' \in \mathbb{Z} \cdot \mathbf{v}$. Furthermore, $\mathbf{f} - \mathbf{f}' = \mathbf{w} - \mathbf{w}'$, and $\mathbf{f} - \mathbf{f}' \in (-1, 1) \cdot \mathbf{v}$; noting that $(-1, 1) \cdot \mathbf{v} \cap \mathbb{Z}\mathbf{v} = \{\mathbf{0}\}$ we conclude that $\mathbf{f} = \mathbf{f}'$ and $\mathbf{w} = \mathbf{w}'$. That is, T is indeed packing. $\square$

Corollary 6 *Let* $\mathbf{B}$ *be a basis of* L*; then* $\mathcal{P}(\mathbf{B}^\star)$ *is a tiling of* L.

Proof: We proceed by induction on the dimension. The base case when $n = 1$ is immediate since then $\mathbf{B}^\star = \mathbf{B}$. Denote $\pi = \pi_{\mathbf{b}_1}$ and let $\mathbf{C} = (\pi(\mathbf{b}_2), \ldots, \pi(\mathbf{b}_n))$ be a basis of $L' = \pi(L)$. Our inductive assumption is that $\mathcal{P}(\mathbf{C}^\star)$ is tiling for $\pi(L)$. By Lemma 5, we have that $\mathcal{P}(\mathbf{C}^\star) + [-1/2, 1/2) \cdot \mathbf{b}_1$ is tiling for L. It remains to note that $\mathbf{b}_1^\star = \mathbf{b}_1$ and that $\mathbf{b}_{i+1}^\star = \mathbf{c}_i^\star$ to conclude that $\mathcal{P}(\mathbf{B}^\star) = \mathcal{P}(\mathbf{C}^\star) + [-1/2, 1/2) \cdot \mathbf{b}_1$ is tiling. $\square$

An important remark is that $\mathcal{P}(\mathbf{B}^\star)$ can be characterized as follow:

$$\mathbf{e} \in \mathcal{P}(\mathbf{B}^\star) \Leftrightarrow \langle \mathbf{e}, \mathbf{b}_i^\star \rangle / \|\mathbf{b}_i^\star\|_2^2 \in [-1/2, 1/2) \text{ for all } i. \tag{1}$$

This characterization is a special case of the argument used in the proof of Lemma 7 from the previous lecture, using the property that $\mathbf{B}^\star$ has orthogonal columns, as in the claim below.

Claim 7 *If $\mathbf{M} \in \mathrm{GL}_n(\mathbb{R})$ has orthogonal columns, then $\mathbf{M}^{-1} = \mathbf{D}^{-1} \cdot \mathbf{M}^\top$ where $\mathbf{D}$ is a diagonal matrix with $d_{i,i} = \|\mathbf{m}_i\|_2^2$.*

Proof: Note that $\mathbf{M}$ having orthogonal columns is equivalent to $\mathbf{M}^\top \cdot \mathbf{M}$ being diagonal. $\square$

In this case, defining $\mathbf{C} = (\mathbf{B}^{\star -1})^\top$, we have $\mathbf{C} = (\mathbf{D}^{-1} \cdot \mathbf{B}^{\star\top})^\top = \mathbf{B}^\star \cdot \mathbf{D}^{-\top} = \mathbf{B}^\star \cdot \mathbf{D}^{-1}$ and conclude that $\mathbf{c}_i = \mathbf{b}_i^\star / \|\mathbf{b}_i\|_2^2$.

Algorithm 1: NearestPlane$(\mathbf{B}, \mathbf{t})$: Nearest Plane Algorithm (Babai)

Input : A basis $\mathbf{B} \in \mathbb{Q}^{n \times n}$ of a full rank lattice Λ, a target $\mathbf{t} \in \mathrm{Span}_{\mathbb{R}}(L)$.
Output: $\mathbf{v} \in L$ such that $\mathbf{e} = \mathbf{t} - \mathbf{v} \in \mathcal{P}(\mathbf{B}^\star)$

```
Compute the GSO B* of B
v ← 0
e ← t
for i = n down to 1 do
    k ← ⌊⟨e, b*_i⟩ / ‖b*_i‖²⌉
    v ← v + k b_i
    e ← v − k b_i
end
return v
```

Lemma 8 *Algorithm 1 is correct and runs in polynomial time.*

Proof: For correctness, we consider various invariants of the **for** loop. First, the equation $\mathbf{v} + \mathbf{e} = \mathbf{t}$ is true at initialization and maintained at each iteration. Secondly, $\mathbf{v} = \mathbf{0}$ at initialization so $\mathbf{v} \in L$, and it remains in L during the loop as we only add integer combination of basis vectors.

We now prove that $\mathbf{e} \in \mathcal{P}(\mathbf{B}^\star)$ at the end of the algorithm. By construction of k, and noting that $|\langle \mathbf{b}_i, \mathbf{b}_i^\star \rangle| = \|\mathbf{b}_i^\star\|^2$, it holds that $|\langle \mathbf{e}, \mathbf{b}_i^\star \rangle| / \|\mathbf{b}_i^\star\|^2 \in [-1/2, 1/2)$ at the end of iteration i. Furthermore, the inner product $\langle \mathbf{e}, \mathbf{b}_i^\star \rangle$ is unaffected by the operation $\mathbf{e} \leftarrow \mathbf{v} - k\mathbf{b}_j$ at later stages of the loop $j < i$ because $\mathbf{b}_j \perp \mathbf{b}_i^\star$ (note crucially that the loop goes by **decreasing** indices i).

We conclude that by the end of the algorithm, it holds that $|\langle \mathbf{e}, \mathbf{b}_i^\star \rangle| / \|\mathbf{b}_i^\star\|^2 \in [-1/2, 1/2)$ for all i, which, by the characterization (1) implies $\mathbf{e} \in \mathcal{P}(\mathbf{B}^\star)$.

Regarding polynomial running time, the algorithm, including the GSO process itself, requires $O(n^3)$ operations over $\mathbb{Q}$, but it remains to analyze how large the numerators and denominators at hand are. We refer the interested reader to Micciancio's Lecture notes.[1] $\square$

[1] `https://cseweb.ucsd.edu/classes/wi10/cse206a/lec2.pdf`

Inner and Outer Radii of $\mathcal{P}(\mathbf{B}^\star)$. Because orthogonal projections and GSO are intimately tied to the Euclidean metric, we will only consider inner and outer radius in the ℓ_2 norm.

For the outer radius we claim that:

$$\mu^{(2)}(\mathcal{P}(\mathbf{B}^\star)) = \frac{1}{2}\sqrt{\sum_{i=1}^{n} \|\mathbf{b}_i^\star\|_2^2}. \tag{2}$$

Indeed, because the $\mathbf{b}_i^\star$ are orthogonal we have Euclidean additivity: $\|\mathbf{B}^\star \cdot \mathbf{x}\|_2^2 = \sum x_i^2 \cdot \|\mathbf{b}_i^\star\|_2^2$. Now since $\mathcal{P}(\mathbf{B}^\star) = \mathbf{B}^\star \cdot [-1/2, 1/2)^n$, the result follows.

At last, using Lemma 7 from the previous lecture and the characterization of orthogonal parallelepiped (1) we can cumpute the inner-radius:

$$\nu^{(2)}(\mathcal{P}(\mathbf{B}^\star)) = \frac{1}{2}\min_{i=1}^{n} \|\mathbf{b}_i^\star\|_2\,. \tag{3}$$