Edoardo Persichetti Lecture 9: Lattices 22/04/2014

Notes written by Łukasz Mazurek

Lattices

Definition 1 (Lattice) Let $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_n$ be linearly independent vectors from $\mathbb{R}^m$. We define a *lattice* as the set

$$L = \{a_1\underline{b}_1 + \ldots + a_n\underline{b}_n \mid a_i \in \mathbb{Z}\}.$$

We also denote the set $B = \{\underline{b}_1, \ldots, \underline{b}_n\}$ by the *basis* of L. The number n is called the *rank* of L, while m is the *dimension* of L. Lattices with $n = m$ are referred to as *full-rank* lattices.

Example 1 For basis $B = \{(1,0),(0,1)\}$, the lattice is actually $\mathbb{Z}^2$. Note that the choice of the basis is not unique, since $B' = \{(1,1),(2,1)\}$ is also the basis of the same lattice. However, $B'' = \{(1,1),(2,0)\}$ forms a different lattice.

Example 2 (not full-rank lattice) A set of points on a line in $\mathbb{R}^2$ formed by basis $B''' = \{(2,1)\}$.

Definition 2 (Discrete subgroup) We call a subgroup L *discrete* if there exists ϵ such that

$$\forall \underline{v} \in L, L \cap \{\underline{w} \in \mathbb{R}^m \mid \|\underline{v} - \underline{w}\| \leq \epsilon\} = \{\underline{v}\}$$

Theorem 1 *The set of discrete subroups of $\mathbb{R}^m$ is equal to the set of lattices in $\mathbb{R}^m$.*

In matrix notation we will write the vectors of basis in rows (equivalently columns), so for a basis $B = \{(1,2),(3,4)\}$ we will write

$$B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Proposition 1 *Let B be the basis of a full-rank lattice L and let B' and U be such matrices that $B' = UB$. Then B' is a basis of L if and only if U is unimodular, i.e.* $\det(U) = \pm 1$.

Proof "$\Rightarrow$": Since B' is another basis of L, U is a non-degenerate matrix of basis change from B to B'. Therefore U^{-1} is a matrix of basis change from B' to B, so

$$B = U^{-1}B' = U^{-1}(UB) = (U^{-1}U)B,$$

so $\det(U^{-1}) \cdot \det(U) = 1$ and hence $\det(U) = 1$ or $\det(U) = -1$.
"$\Leftarrow$" (Sketch): We will only explain in detail the case where U is a permutation matrix. In this case, the lattice formed by B' is equal to

$$L' = \{\underline{a}B' \mid \underline{a} \in \mathbb{Z}^n\} = \{\underline{a}UB \mid \underline{a} \in \mathbb{Z}^n\} = \{\underline{a}'B \mid \underline{a}' \in \mathbb{Z}^n\} = L$$

Proposition 2 *Let $B = \{\underline{b}_1, \ldots, \underline{b}_n\}$ be a $\mathbb{R}^{n\times m}$ matrix denoting the basis of a non-full-rank lattice. Then, there exists a transformation $P : \mathbb{R}^m \to \mathbb{R}^n$ such that*

- *$P(L)$ is a full-rank lattice of rank n,*
- *$\forall \underline{v} \in L, \|P(\underline{v})\| = \|\underline{v}\|$,*
- *$\forall i, j \leq n, \langle \underline{b}_i, \underline{b}_j \rangle = \langle P(\underline{b}_i), P(\underline{b}_j) \rangle$,*

Where $\|\underline{x}\|$ denotes an Euclidean norm $\|\underline{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$. Note that since P can be represented as a $m \times n$ matrix, we can use the notation $P(\underline{v}) = \underline{v}P$. Then P transforms the basis B into a new $n \times n$ basis $B' = BP$.

Proof Let $V = \text{span}\{\underline{b}_1, \ldots, \underline{b}_n\} \subset \mathbb{R}^m$. Denote by $V' = \{\underline{v}_1, \ldots, \underline{v}_n\}$ the orthonormal basis obtained from $\{b_1, \ldots, b_n\}$ during the Gram-Schmidt orthonormalisation procedure. We take the following $P : V \to \mathbb{R}^n$:

- $P(\underline{v}_i) = \underline{e}_i$ for $i = 1, \ldots, n$,
- $P(V^\perp) = \underline{0}$.

For a general $\underline{v} = \sum_{i=1}^n a_i \underline{v}_i \in V$ we have

$$\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle} = \sqrt{\sum_{i=1}^n a_i^2 \|v_i\|^2} = \sqrt{\sum_{i=1}^n a_i^2}.$$

On the other hand

$$\|\underline{v}P\| = \|P(\underline{v})\| = \left\| \sum_{i=1}^n a_i \underline{e}_i \right\| = \sqrt{\sum_{i=1}^n a_i^2},$$

so $\|\underline{v}\| = \|\underline{v}P\|$.
The last equality $\langle b_i, b_j \rangle = \langle P(b_i), P(b_j) \rangle$ follows simply from the fact, that $\langle \underline{b}_i, \underline{b}_j \rangle = \langle P(\underline{b}_i), P(\underline{b}_j) \rangle = [i = j]$.
Lastly, because $\{\underline{b}_1, \ldots, \underline{b}_n\}$ forms a basis, all vectors $P(\underline{b}_i)$ are linearly independent, so BP is invertible and $P(L)$ is a full-rank lattice of rank n.

Corollary 1 *Proposition 1 holds also for non-full-rank lattices.*

Kernel lattice

The kernel of a linear map $A : \mathbb{R}^m \to \mathbb{R}^n$ restricted to integer vectors $\{\underline{a} \in \mathbb{Z}^m : \underline{a}A = \underline{0}\}$ forms a lattice.

Hermite Normal Form (HNF)

The Hermite Normal Form (HNF) of a matrix is a non-negative matrix with

- positive elements on the diagonal,
- zeros below the diagonal,
- elements smaller then $a_{i,i}$ above $a_{i,i}$ in the i-th column.

More formally:

Definition 3 A matrix A is in *HNF* form if there exists a number r and a strictly increasing function f such that

1. first r columns are filled with zeros,
2. $f(\{r+1,\ldots,n\}) = \{1,\ldots,m\}$,
3. $\forall j \in \{r+1,\ldots,n\}, 0 \leq A_{i,j} < A_{f(j),j}$ for $i < f(j)$,
4. $A_{f(i),i} > 0$ for $1 \leq i \leq n$,
5. $A_{i,j} = 0$ if $i > f(j)$.

Definition 4 A lattice with all basis vectors in $\mathbb{Z}^m$.

Integral lattice

The Determinant of a Lattice

Definition 5 The *determinant* of a lattice is equal to the volume of the parallelepiped formed by its basis vectors.

Example 3 If $n = m = 2$ and $B = \{\underline{b}_1, \underline{b}_2\}$ is a basis of a lattice L, then $\det(L) = \|\underline{b}_1\|\|\underline{b}_2\| \sin\theta$, where θ is the angle between $\underline{b}_1$ and $\underline{b}_2$. Given the lengths of basis vectors, the determinant is maximized for $\underline{b}_1 \perp \underline{b}_2$.

In general, the determinant of a lattice satisfies the *Hadamard inequality*:

$$\det(L) \leq \|\underline{b}_1\| \cdots \|\underline{b}_n\|.$$

Theorem 2 *Let L be a lattice with basis B. Then the determinant of L satisfies*

$$\det(L) = \begin{cases} |\det(B)| & \textit{(full-rank lattice)} \\ |\det(BP)| & \textit{(non-full-rank lattice)} \end{cases}.$$

The value of the determinant does not depend on

1. *choice of the basis B,*
2. *choice of the projection matrix P for non-full-rank lattices.*

Proof (1) For any basis B' let U be an unimodular matrix, such that $B' = BU$. Then $\det(U) = \pm 1$ and $|\det(B')| = |\det(BU)|$

(2) Let $V = \text{span}\{\underline{b}_1,\ldots,\underline{b}_n\}$, $P = \{\underline{v}_1,\ldots,\underline{v}_n\}$, $P' = \{\underline{v}'_1,\ldots,\underline{v}'_n\}$, where $P' = PW$, W is an orthogonal matrix and $\det(W) = \pm 1$. Then $|\det(BP')| = |\det(BPW)| = |\det(BP)|$.

Computational problems on lattices

Easy problems

Lattice membership Given a basis B for a lattice L and a vector $\underline{v} \in \mathbb{Z}^m$, determine if $\underline{v} \in L$ (easy with HNF).

Lattice basis Given n vectors from a lattice L, find the basis for L.

Kernel lattice Given a linear map A, find a kernel lattice $L = \ker(A)$.

Hard problems

I Shortest Vector Problem (SVP) Given the basis B for a lattice L, compute a non-zero vector $\underline{v} \in L$, such that $\|\underline{v}\|$ is minimal ($\underline{v}$ can be non-unique).

II Closest Vector Problem (CVP) Given the basis B for a lattice L and a vector $\underline{w} \in \mathbb{R}^m$, compute a vector $\underline{v} \in L$, such that $\|\underline{v} - \underline{w}\|$ is minimal.

I a) Decisional Shortest Vector Problem (DSVP) Given the basis B for a lattice L and a real number r, determine if there exists a non-zero vector $\underline{v} \in L$, such that $\|\underline{v}\| < r$.

II a) Decisional Closest Vector Problem (CVP) Given the basis B for a lattice L, a vector $\underline{w} \in \mathbb{R}^m$ and a real number r, determine if there exists a vector $\underline{v} \in L$, such that $\|\underline{v} - \underline{w}\| < r$.

I b) Approximate Shortest Vector Problem (ASVP) Given the basis B for a lattice L and a fixed security parameter $\gamma > 1$, determine if there exists a non-zero vector $\underline{v} \in L$, such that $\|\underline{v}\| < \gamma\|\underline{a}B\|$ for all $\underline{a} \in \mathbb{Z}^m$.

II b) Approximate Closest Vector Problem (ACVP) Given the basis B for a lattice L, a vector $\underline{w} \in \mathbb{R}^m$ and a fixed security parameter $\gamma > 1$, determine if there exists a non-zero vector $\underline{v} \in L$, such that $\|\underline{v} - \underline{w}\| < \gamma\|\underline{a}B - \underline{w}\|$ for all $\underline{a} \in \mathbb{Z}^m$.

Remark 1 If the basis is "too nice", e.g. is orthogonal, then the problems become easy:

Example 4 Consider a lattice $L \subset \mathbb{R}^2$ and formed by the orthogonal basis

$$B = \begin{pmatrix} 1001 & 0 \\ 0 & 2008 \end{pmatrix}.$$

The lattice L can be described as a set of points $L = \{(1001a, 2008b) \mid a, b \in \mathbb{Z}\}$. It is easy to see that the shortest vectors are $(1001, 0)$ and $(-1001, 0)$.

Example 5 For the same basis and a vector $\underline{w} = (5432, 6000)$, it is easy to find the closest vector $\underline{v} = (5005, 6024)$.

Informally speaking, *the less orthogonal* the basis is, the harder the problems becomes.

Hermite's theorem

Theorem 3 (Hermite) *For every lattice $L \subset \mathbb{R}^n$ there exists a vector $\underline{v} \in L$ such that*

$$\|v\|^2 \leq \gamma_n \det(L)^{2/n},$$

where γ_n is called Hermite's constant. *It is known that $\gamma_n \leq n$. The exact value of γ_n has only been calculated for the first 8 values (plus γ_{24}), but for large enough n it satisfies:*

$$\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e}.$$

Corollary 2 *For every lattice $L \subset \mathbb{R}^n$ there exists a vector $\underline{v} \in L$ such that*

$$\|v\| \leq \sqrt{n} \det(L)^{1/n}.$$

Corollary 3 *For every lattice $L \subset \mathbb{R}^n$ there exists a basis $\underline{v}_1, \ldots, \underline{v}_n \in L$ such that*

$$\|\underline{v}_1\| \cdots \|\underline{v}_n\| \leq n^{n/2} \det(L).$$

Definition 6 We define the Hadamard ratio of a lattice L with basis B as

$$H(B) = \left(\frac{\det(L)}{\|\underline{v}_1\| \cdots \|\underline{v}_n\|} \right)^{1/n}.$$

From the Hadamard inequality we get that

$$0 < H(B) \leq 1.$$

The Hadamard ratio measures the "orthogonality" of a basis in the following way: the closer $H(B)$ is to 1, the closer the basis is to orthogonal. Alternatively it is possible to use the notion of *orthogonality defect*, which is equal to $1/H(B)$.

Technical tool: Minkovski's Convex Body Theorem

In this section we formulate without proof the Minkovski's Convex Body Theorem, which will be used to prove Hermite's theorem.

Definition 7 For any $\underline{a} \in \mathbb{R}^n$ and $R > 0$ we define the n-dimensional ball centered in $\underline{a}$ of radius R as:

$$B_R(\underline{a}) = \{\underline{x} \in \mathbb{R}^n \mid \|\underline{x} - \underline{a}\| \leq R\}.$$

Definition 8 A subset $S \subset \mathbb{R}^n$ is *bounded* if there exists a constant λ such that

$$\forall \underline{v} \in S, \|\underline{v}\| < \lambda$$

or equivalently

$$\exists R | S \subset B_R(\underline{0}).$$

Definition 9 A subset $S \subset \mathbb{R}^n$ is *symmetric* if for all $\underline{v} \in \mathbb{R}^n$

$$\underline{v} \in S \implies -\underline{v} \in S.$$

Definition 10 A subset $S \subset \mathbb{R}^n$ is *convex* if for all $\underline{a}, \underline{b} \in S$, the segment connecting $\underline{a}$ to $\underline{b}$ is all contained in S.

Theorem 4 (Minkovski's Convex Body Theorem) *Let $L \subset \mathbb{R}^n$ be a lattice and $S \subset R^n$ be a symmetric and convex set such that*

$$\mathrm{Vol}(S) > 2^n \det(L).$$

Then there exists a non-zero vector $\underline{v}$ such that $\underline{v} \in S \cap L$. Furthermore, if S is closed, the thesis holds for

$$\mathrm{Vol}(S) \geq 2^n \det(L).$$

Proof of Hermite's theorem Let $L \subset \mathbb{R}^n$ be a lattice. Let S be a hypercube centered in $\underline{0}$ with sides of length $2B = 2\det(L)^{1/n}$:

$$S = \{(a_1, \ldots, a_n) \in \mathbb{R}^n \mid -B \leq a_i \leq B\}.$$

It is easy to see that S is symmetric, convex and bounded and $\mathrm{Vol}(S) = 2^n \det(L)$. Using Minkovski's theorem, there exists a non-zero vector $\underline{a} \in S \cap L$. Then

$$\|\underline{a}\| = \sqrt{a_1^2 + \cdots + a_n^2} \leq \sqrt{n}B = \sqrt{n}\det(L)^{1/n},$$

which ends the proof (the inequality $\sqrt{a_1^2 + \cdots + a_n^2} \leq \sqrt{n}B$ follows from the fact, that $\underline{a}$ is a vector inside a hypercube centered in $\underline{0}$ with sides of length $2B$).

Remark 2 A better bound can be obtained via the *Gaussian Heuristic*, a similar but more complex method which applies the technique described above to a hypersphere instead of a hypercube. In this case the expected length of the shortest vector of the lattice is approximately equal to

$$\sigma(L) = \sqrt{\frac{n}{2\pi e}}\det(L)^{1/n}.$$