UNIVERSITÉ DU LUXEMBOURG

Introduction to lattices

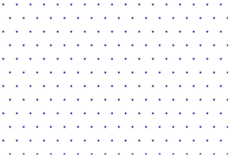
Barthel Jim

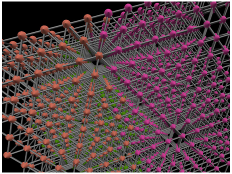
May 24, 2019

Luxembourg National Research Fund

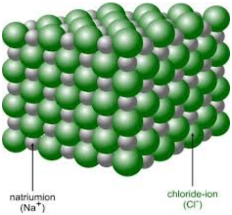
Supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

What is a lattice?





http://www.gracebyte.com/lattice/images/ss_2.jpg



https://docplayer.nl/19815420-Hoofdstuk-4-atoombouw-en-periodiek-systeem.html

http://www.aamt.edu.au/digital-resources/R10266/index.html

Table of contents

Part I:

Definitions

The formal definition of a lattice

Definition (lattice)

A *lattice* is a discrete additive subgroup of $\mathbb{R}^n$.
In other words, a *lattice* is a subset $\Lambda \subseteq \mathbb{R}^n$ satisfying the following properties:

1. (Subgroup property) Λ is closed under addition and subtraction.
2. (Discreteness) There is an $\epsilon > 0$ such that any two distinct lattice points $x \neq y \in \Lambda$ are at distance at least $\|x - y\| \geq \epsilon$.

Constructing lattices

Definition 1 (lattice generated by linearly independent vectors)

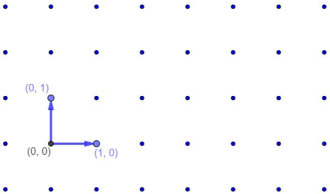
Let $b_1, ..., b_n \in \mathbb{R}^m$ be linearly independent vectors.
Let $B = [b_1, ..., b_n]$.

1. The lattice *generated by* B is the set

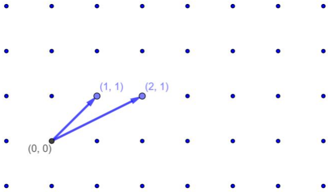
$$\mathcal{L}(B) = \{Bx \in \mathbb{Z}^m : x \in \mathbb{Z}^n\} = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

2. The matrix B is called the *basis* of the lattice $\mathcal{L}(B)$.
3. We call n the *rank* of $\mathcal{L}(B)$ and m the *dimension* of $\mathcal{L}(B)$.
4. If $n = m$, then $\mathcal{L}(B)$ is called a *full rank* lattice.

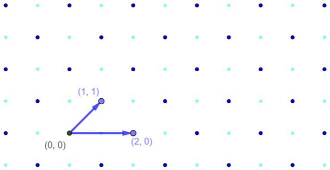
Examples of lattices



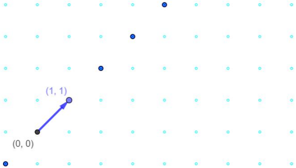
A basis of $\mathbb{Z}^2$



Another basis of $\mathbb{Z}^2$



Not a basis of $\mathbb{Z}^2$



Not a full-rank lattice

Definitions emerging from lattices

Definition 2

Let B be any lattice basis and let $\mathcal{L}(B)$ be the corresponding lattice.

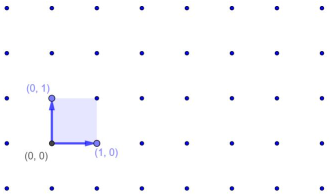
1. The *span* of $\mathcal{L}(B)$ is the vector space generated by B:

$$span(\mathcal{L}(B)) = span(B) =< B >= \{Bx \in \mathbb{R}^m : x \in \mathbb{R}^n\}$$

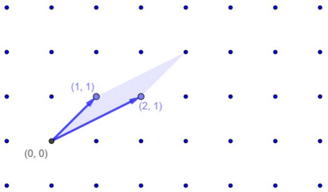
2. The fundamental parallelepiped of the lattice basis B is given by

$$P(B) = \{Bx \in \mathbb{R}^m : x \in \mathbb{R}^n,\ 0 \leq x_i < 1 \quad \forall 0 \leq i \leq n\}$$
$$= \left\{ \sum_{i=1}^{n} x_i b_i : 0 \leq x_i < 1 \right\}.$$

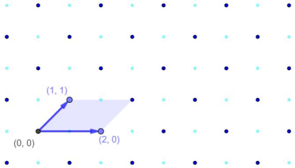
More examples



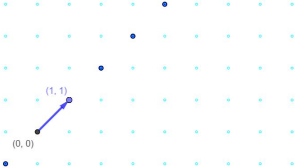
A basis of $\mathbb{Z}^2$



Another basis of $\mathbb{Z}^2$



Not a basis of $\mathbb{Z}^2$



Not a full-rank lattice

Part II:

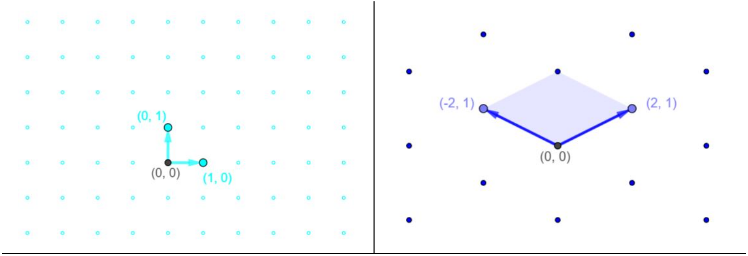
Comparing lattices

A lattice and its possible bases (1)

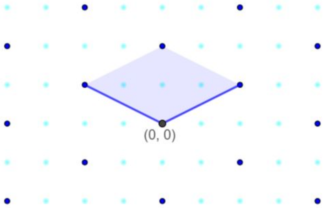
Lemma 3

Let Λ be a lattice of rank n, and let $b_1, ..., b_n \in \Lambda$ be linearly independent lattice vectors.
Then, $b_1, ..., b_n$ form a basis of $\Lambda \Leftrightarrow P(b_1, ..., b_n) \cap \Lambda = \{0\}$.

A lattice and its possible bases (2)



We compare both lattices by superposing them:



A lattice and its possible bases (3)

Proof of lemma 3:

1) $b_1, ..., b_n$ form a basis of $\Lambda \Rightarrow P(b_1, ..., b_n) \cap \Lambda = \{0\}$:

- By definition,

$$\Lambda = \left\{ \sum x_i b_i : x_i \in \mathbb{Z} \right\}.$$

- Furthermore,

$$P(b_1, ..., b_n) = \left\{ \sum x_i b_i : 0 \leq x_i < 1 \right\}.$$

- Hence,

$$P(b_1, ..., b_n) \cap \Lambda = \{0\}.$$

A lattice and its possible bases (4)

2) $P(b_1, ..., b_n) \cap \Lambda = \{0\} \Rightarrow b_1, ..., b_n$ form a basis of Λ:

1. Since $b_1, ..., b_n \in \Lambda$, $\mathcal{L}(b_1, ..., b_n) \subseteq \Lambda$.
2.
   - Since Λ is a lattice of rank n and $b_1, ..., b_n$ are n linearly independent lattice vectors of Λ,
   $$\forall x \in \Lambda : x = \sum x_i b_i \ (x_i \in \mathbb{R}).$$
   - Let
   $$x' = \sum \lfloor x_i \rfloor b_i \in \Lambda.$$
   - Let
   $$x'' = x - x' = \sum (x_i - \lfloor x_i \rfloor) b_i.$$
   - Since Λ is closed under addition and subtraction
   $$x'' \in \Lambda.$$
   - Since $0 \leq x_i - \lfloor x_i \rfloor < 1$ for all $1 \leq i \leq n$,
   $$x'' \in P(b_1, ..., b_n).$$

A lattice and its possible bases (4)

2) $P(b_1, ..., b_n) \cap \Lambda = \{0\} \Rightarrow b_1, ..., b_n$ form a basis of Λ:

1. Since $b_1, ..., b_n \in \Lambda$, $\mathcal{L}(b_1, ..., b_n) \subseteq \Lambda$.
2.
   - Since Λ is a lattice of rank n and $b_1, ..., b_n$ are n linearly independent lattice vectors of Λ,

   $$\forall x \in \Lambda : x = \sum x_i b_i \ (x_i \in \mathbb{R}).$$

   - Let

   $$x' = \sum \lfloor x_i \rfloor b_i \in \Lambda.$$

   - Let

   $$x'' = x - x' = \sum (x_i - \lfloor x_i \rfloor) b_i \in P(b_1, ..., b_n) \cap \Lambda.$$

   - Since $P(b_1, ..., b_n) \cap \Lambda = \{0\}$, $x'' = 0$.
   - Since $b_1, ..., b_n$ are linearly independent,

   $$x_i = \lfloor x_i \rfloor \text{ for all} 1 \leq i \leq n.$$

   In particular x_i is an integer for all $1 \leq i \leq n$.
   - Hence, $x \in \mathcal{L}(b_1, ..., b_n)$ and so

   $$\Lambda \subseteq \mathcal{L}(b_1, ..., b_n).$$

Equivalence of bases (1)

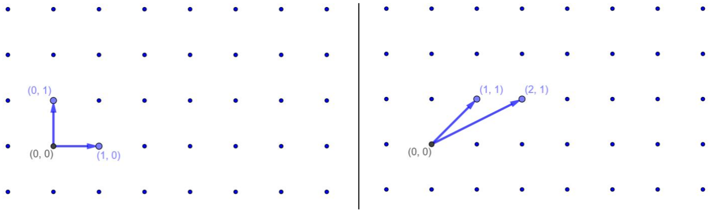
Definition 4 (equivalence of lattices)

Let B_1, B_2 be lattice bases. We say that B_1 is *equivalent* to B_2 if and only if $\mathcal{L}(B_1) = \mathcal{L}(B_2)$.

Lemma 5

Two bases B_1, B_2 of rank n are equivalent if and only if there exists an unimodular matrix U (i.e. U is a square matrix with integer coefficients and $\det(U) = \pm 1$) such that $B_2 = B_1 U$.

Equivalence of bases (2)



Note that

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

and that

$$\det \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = -1.$$

Equivalence of bases (3)

Proof of lemma 5:

1) B_1, B_2 are equivalent $\Rightarrow \exists U$ unimodular such that $B_2 = B_1 U$:

- Since B_1 and B_2 are equivalent,
$$\mathcal{L}(B_1) = \mathcal{L}(B_2).$$
- Since $\forall 1 \leq i \leq n : b_i \in B_2$,
$$b_i \in \mathcal{L}(B_2) = \mathcal{L}(B_1).$$
- By definition of the lattice $\mathcal{L}(B_1)$,
$$\exists u_i \in \mathbb{Z}^n \text{ such that } b_i = B_1 u_i.$$
- Let $U = (u_1, ..., u_n)$. Then clearly,
$$B_2 = B_1 U.$$
- Similarly, one can construct $V \in \mathbb{Z}^{n \times n}$ such that
$$B_1 = B_2 V.$$

Equivalence of bases (3)

Proof of lemma 5:

1) B_1, B_2 are equivalent $\Rightarrow \exists U$ unimodular such that $B_2 = B_1 U$:

- We deduce that $B_2 = B_2 V U$ and so

$$B_2(Id - VU) = 0.$$

- Since the column vectors of B_2 are linearly independent, its inverse exists and so

$$Id = VU.$$

- Since $1 = \det(Id) = \det(V)\det(U)$ and U, V are integer matrices,

$$\det(U) = \pm 1.$$

Equivalence of bases (4)

2) $\exists U$ unimodular such that $B_2 = B_1 U \Rightarrow B_1, B_2$ are equivalent:

- Since $B_2 = B_1 U$ where $B_2 = (b_1, ..., b_n)$ and $U = (u_1, ..., u_n)$,
$$\forall 1 \leq i \leq n: \; b_i = B_1 u_i.$$
- Since U is unimodular, $b_i \in \mathcal{L}(B_1)$ and hence
$$\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1).$$
- Since any unimodular matrix has an inverse which is also unimodular, we first deduce that
$$B_1 = B_2 U^{-1}.$$
and then, the same argument as above yields
$$\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2).$$

Deducing one basis from another one

Corollary 6

Two bases are equivalent if and only if one can be obtained from the other by the following operations on columns:

1. $b_i \leftarrow b_i + k b_j$ for some $k \in \mathbb{Z}$ and $i \neq j$,
2. $b_i \leftrightarrow b_j$,
3. $b_i \leftarrow -b_i$.

Part III:

Gram-Schmidt Orthogonalization

Gram-Schmidt orthogonalization

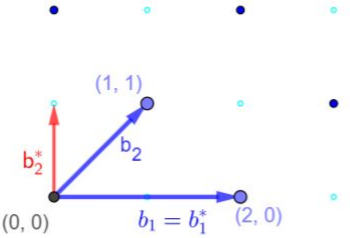
Definition 7 (Gram-Schmidt orthogonalization)

Given any sequence of n linearly independent vectors $b_1, ..., b_n \in \mathbb{R}^m$, we define their *Gram-Schmidt orthogonalization* as the sequence of vectors $b_1^*, ..., b_n^* \in \mathbb{R}^m$ defined recursively by

$$b_i^* = b_i - \sum_{j=1}^{i-1} \frac{< b_i, b_j^* >}{< b_j^*, b_j^* >} b_j^*.$$

In other words, b_i^* is the component of b_i orthogonal to $b_1^*, ..., b_{i-1}^*$.

An example of Gram-Schmidt



The vector b_2^* does not belong to the lattice.

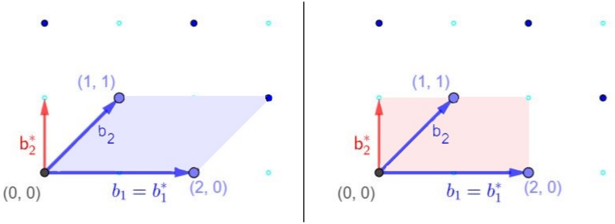
Properties of Gram-Schmidt orthogonalization

Remark 8

Let $b_1, ..., b_n \in \mathbb{R}^m$ be n linearly independent vectors and let $b_1^*, ..., b_n^* \in \mathbb{R}^m$ be their Gram-Schmidt orthogonalization.

1. (Orthogonality) For all $i \neq j$ we have $< b_i^*, b_j^* >= 0$.
2. (Basis) For all $1 \leq i \leq n$,
   $span(b_1, ..., b_i) = span(b_1^*, ..., b_i^*)$.
   Note that in general $\mathcal{L}(b_1, ..., b_n) \neq \mathcal{L}(b_1^*, ..., b_n^*)$ (most of the time $b_i^* \notin \mathcal{L}(b_1, ..., b_n)$) and that a lattice does not always admit an orthogonal basis!
3. (Order) The order of the Gram-Schmidt procedure matters.

Volume of the fundamental parallelepiped



$$vol(P(b_1, b_2)) = \|b_1^*\| \, \|b_2^*\| = 2$$

Remark 9

Let $b_1, ..., b_n \in \mathbb{R}^m$ be n linearly independent vectors and let $b_1^*, ..., b_n^* \in \mathbb{R}^m$ be their Gram-Schmidt orthogonalization. Then:

$$vol(P(b_1, ..., b_n)) = \prod_{i=1}^{n} \|b_i^*\|.$$

Part IV:

Determinant

Determinant

Definition 10 (determinant of lattices)

Let $\Lambda = \mathcal{L}(B)$ be a lattice of rank n. We define the *determinant* of Λ (denoted by $\det(\Lambda)$) to be the n-dimensional volume of the fundamental parallelepiped $P(B)$ associated to B. In symbols:

$$\det(\Lambda) = vol(P(B)) = \prod_{i=1}^{n} \|b_i^*\|.$$

Properties of the determinant (1)

Proposition 11

For any lattice basis $B \in \mathbb{R}^{n \times m}$

1. $\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)}$,
2. In particular if $B \in \mathbb{R}^{n \times n}$ is a (non-singular) square matrix, then $\det(\mathcal{L}(B)) = |\det(B)| = d$ and $d\mathbb{Z}^n \subseteq \mathcal{L}(B)$.
3. The determinant is independent of the basis.

Properties of the determinant (2)

Proof of proposition 11:

1) $\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)}$:

- By the Gram-Schmidt orthogonalization procedure, we know that
$$B = B^* M$$
where M is an upper triangular matrix with 1's on the diagonal and $\frac{<b_i, b_j^*>}{<b_j^*, b_j^*>} \|b_j^*\|$ for all $j < i$.
- Hence,
$$\sqrt{\det(B^T B)} = \sqrt{\det(M^T (B^*)^T B^* M)} = \sqrt{\det(M^T) \det((B^*)^T B^*) \det(M)}.$$
- Since M is upper triangular and has only 1's at its diagonal,
$$\det(M) = \det(M^T) = 1.$$
- Furthermore, by orthogonality of the columns of B^*,
$$\det((B^*)^T B^*) = \prod_{i=1}^{n} (\|b_i^*\|)^2 = (\det(\mathcal{L}(B)))^2.$$
- Since $\det(\mathcal{L}(B)) \geq 0$ by definition,
$$\sqrt{\det((B^*)^T B^*)} = \det(\mathcal{L}(B)).$$

Properties of the determinant (3)

2) If $B \in \mathbb{R}^{n \times n}$ is a (non-singular) square matrix, then $\det(\mathcal{L}(B)) = |\det(B)| = d$ and $d\mathbb{Z}^n \subseteq \mathcal{L}(B)$.

- Since B is a square matrix,

$$\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)} = \sqrt{(\det(B))^2} = |\det(B)|.$$

- Let $v = dy \in d\mathbb{Z}^n$ where $y \in \mathbb{Z}^n$.
- Since B is non-singular, there is

$$x = B^{-1} dy \in \mathbb{R}^n.$$

- By Cramer's rule:

$$x_i = \frac{\det((b_1, ..., b_{i-1}, dy, b_{i+1}, ..., b_n))}{\det(B)}$$
$$= \pm \det((b_1, ..., b_{i-1}, dy, b_{i+1}, ..., b_n)) \in \mathbb{Z}$$

- Thus,

$$x \in \mathbb{Z}^n.$$

- Hence,

$$v = Bx \in \mathcal{L}(B).$$

Properties of the determinant (4)

3) The determinant is independent of the basis.

- Let B_1, B_2 be equivalent bases. Then, there is a unimodular matrix U such that
$$B_2 = B_1 U.$$
- Thus,
$$\begin{aligned}
\det(\mathcal{L}(B_2)) &= \sqrt{\det(B_2^T B_2)} \\
&= \sqrt{\det(U^T B_1^T B_1 U)} \\
&= \sqrt{(\det(U))^2 \det(B_1^T B_1)} \\
&= \sqrt{\det(B_1^T B_1)} \\
&= \det(\mathcal{L}(B_1))
\end{aligned}$$

Remarks about the determinant

Remark 12

For any lattice basis $B \in \mathbb{R}^{n \times m}$

1. (Hadamar inequality)

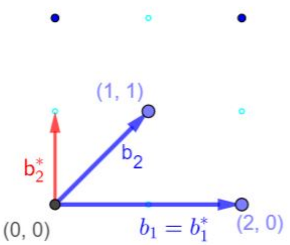
$$\det(\mathcal{L}(B)) = \prod_{i=1}^{n} \|b_i^*\| \leq \prod_{i=1}^{n} \|b_i\|$$

(since $\|b_i^*\| \leq \|b_i\|$).

2. Geometrically, the determinant represents the inverse of the density of lattice points in space (e.g., the number of lattice points in a large and sufficiently regular region of space A should be approximately equal to the volume of A divided by the determinant.)

Small determinant = Dense lattice

An example of a determinant

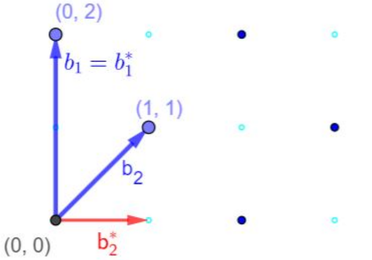


By previous computations:

$$\det(\mathcal{L}(b_1, b_2)) = \|b_1^*\| \; \|b_2^*\| = 2$$

Hadamar's inequality is satisfied:

$$\det(\mathcal{L}(b_1, b_2)) \leq 2\sqrt{2} = \|b_1\| \; \|b_2\|$$



$$\det\left(\mathcal{L}\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}\right) = \sqrt{\det\left(\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}\right)} = \sqrt{\det\left(\begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}\right)} = 2$$

Note

$$\det\left(\mathcal{L}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1$$

Hence, $\mathcal{L}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (i.e. dark and light blue points) is denser than $\mathcal{L}\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$.

Part V:

Successive minima

Sucessive minima (1)

Definition 13a (minimum distance)

Let $\Lambda = \mathcal{L}(B)$ be a lattice of rank n.
The *minimum distance* λ_1 of Λ is the smallest distance between any two lattice points:

$$\lambda_1(\Lambda) = \inf\{\|x - y\| : x, y \in \Lambda, x \neq y\}.$$

Equivalently, the *minimum distance* can be defined as the shortest non-zero vector of Λ:

$$\lambda_1(\Lambda) = \inf\{\|v\| : v \in \Lambda \setminus \{0\}\}.$$

Equivalently, the *minimum distance* is the smallest $r > 0$ such that Λ contains at least one vector of length bounded by r,

$$\lambda_1(\Lambda) = \inf\{r \in \mathbb{R}_{>0} : \dim(span(\Lambda \cap B(0, r))) \geq 1\}$$

where $B(0, r) = \{x \in \mathbb{R}^m : \|x\| \leq r\}$ is the closed ball of radius r around 0.

Sucessive minima (2)

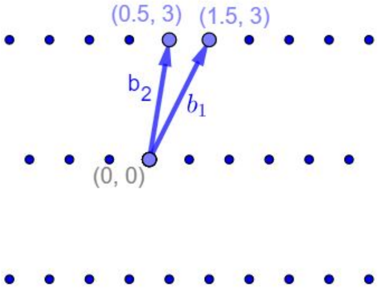
Definition 13b (successive minima)

Let $\Lambda = \mathcal{L}(B)$ be a lattice of rank n.
For $i \in \{1, ..., n\}$, we define the i^{th} *successive minimum* as the smallest $r > 0$ such that Λ contains at least i linearly independent vectors of length bounded by r,

$$\lambda_i(\Lambda) = \inf\{r \in \mathbb{R}_{>0} : \dim(span(\Lambda \cap B(0, r))) \geq i\}$$

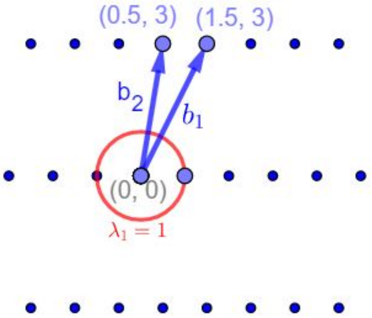
where $B(0, r) = \{x \in \mathbb{R}^m : \|x\| \leq r\}$ is the closed ball of radius r around 0.

An example of successive minima



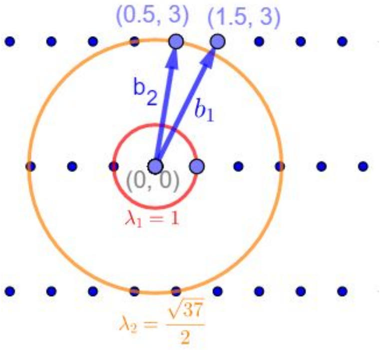
Consider $\mathcal{L}\begin{pmatrix} 1/2 & 3/2 \\ 3 & 3 \end{pmatrix}$.

An example of successive minima



Start to grow a circle at the origin until you meet a point to find λ_1.

An example of successive minima



Keep growing the circle until you meet a second point that lies not on the line given by the minimal vector to find λ_2.

Rough lower bound (1)

Theorem 14

Let B be a rank n lattice basis and let B^* be its Gram-Schmidt orthogonalization. Then:

$$\lambda_1(\Lambda) \geq \min_{i=1,\dots,n} \|b_i^*\| > 0.$$

Thus, for any two non-equal lattice points $x, y \in \Lambda$

$$\|x - y\| \geq \min_{i=1,\dots,n} \|b_i^*\| > 0$$

Rough lower bound (2)

Proof of theorem 14:

- Let,

$$Bx \in \mathcal{L}(B) \setminus \{0\}$$

  be a generic lattice vector where $x \in \mathbb{Z}^n \setminus \{0\}$.

- Let

$$k = \max\{k \in \{1, ..., n\} : x_k \neq 0\}.$$

- Then, by orthogonality

$$| < Bx, b_k^* > | = \left| \sum_{i \leq k} < b_i x_i, b_k^* > \right| = |x_k < b_k, b_k^* > | = |x_k| \|b_k^*\|^2.$$

- By Cauchy-Schwartz,

$$| < Bx, b_k^* > | \leq \|Bx\| \; \|b_k^*\|.$$

- Since $|x_k| \geq 1$ and $\|b_k^*\| \neq 0$,

$$\|b_k^*\| \leq \|Bx\|.$$

The successive minima are achieved (1)

Theorem 15

The successive minima of a lattice are achieved.
In other words, for every $1 \leq i \leq n$, there exists a vector $v_i \in \Lambda$ with $\|v_i\| = \lambda_i(\Lambda)$.

The successive minima are achieved (2)

Proof of theorem 14:

- Let,
$$S = B(0, 2\lambda_1(\Lambda)) = \{x \in R^m : \|x\| < 2\lambda_1(\Lambda)\}.$$
- By definition of the minimal distance, there is at least one lattice point $x \in S$.
- Thus,
$$\lambda_1(\Lambda) = \inf\{\|x\| : x \in \Lambda \cap S \setminus \{0\}\}.$$
- Consider a small sphere of radius $\frac{1}{2}\lambda_1(\Lambda)$ around each lattice point:
$$B\left(x, \frac{1}{2}\lambda_1(\Lambda)\right) \text{ for all } x \in \Lambda.$$
- Since the minimal distance between lattice points is $\lambda_1(\Lambda)$,
$$B\left(x, \frac{1}{2}\lambda_1(\Lambda)\right) \cap B\left(y, \frac{1}{2}\lambda_1(\Lambda)\right) = \emptyset \text{ for all } x \neq y \in \Lambda.$$
- For all $x \in S \cap \Lambda$,
$$B\left(x, \frac{1}{2}\lambda_1(\Lambda)\right) \subseteq B(0, 3\lambda_1(\Lambda)) = S'.$$

The successive minima are achieved (3)

- Notice that:

$$vol\left(B\left(x, \frac{1}{2}\lambda_1(\Lambda)\right)\right) = C_n\left(\frac{1}{2}\lambda_1(\Lambda)\right)^n \text{ and}$$

$$vol(0, 3\lambda_1(\Lambda)) = C_n(3\lambda_1(\Lambda))^n$$

- Hence, there are at most 6^n lattice points in S. So,

$$\lambda_1(\Lambda) = \inf\{\|x\| : x \in \Lambda \cap S \setminus \{0\}\} = \min\{\|x\| : x \in \Lambda \cap S \setminus \{0\}\}.$$

- By a similar argument, one proves the theorem for the other successive minima.

Part VI:

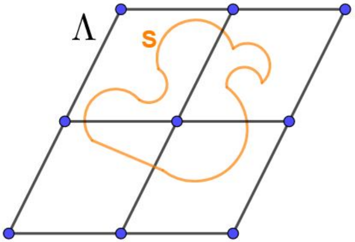
Minkowski's theorems

Blichfeld's theorem (1)

Theorem 16 (Blichfeld)

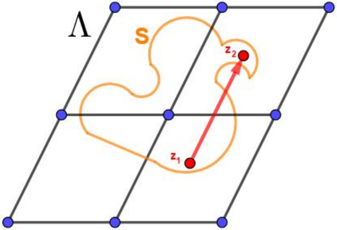
Let $\Lambda = \mathcal{L}(B) \subseteq \mathbb{R}^n$ be a full-rank lattice and let $S \subseteq \mathbb{R}^n$ be a subset with $vol(S) > \det(\Lambda)$. Then, there exist two nonequal points $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.

Blichfeld example



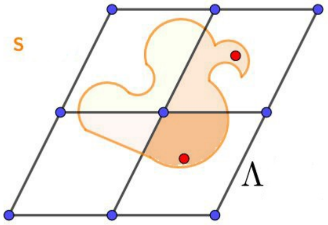
Consider the lattice Λ and $S \subseteq \mathbb{R}^n$ with $vol(S) > \det(\Lambda)$.

Blichfeld example



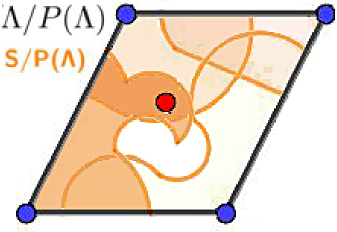
Then, we want to find $z_1, z_2 \in S$ such that $z_1 - z_2 \in \Lambda$.

Blichfeld example



To do so, consider $\mathbb{R}^2$ partitioned by the lattice.

Blichfeld example



Reduce all of $\mathbb{R}^2$ to the fundamental parallelepiped and look for intersections, this gives us the two points we are looking for.

Blichfeld's theorem (2)

Proof of theorem 16:

- As x ranges over all of Λ, we can partition $\mathbb{R}^n$ by considering the sets
$$x + P(B) = \{x + y : y \in P(B)\}.$$
- For any $x \in \Lambda$, define
$$S_x = S \cap (x + P(B)).$$
- Since $x + P(B)$ partitions $\mathbb{R}^n$, it does so with S. Hence,
$$S_x \cap S_y = \emptyset \ (\forall x \neq y) \text{ and } S = \cup_{x \in \Lambda} S_x.$$
- This implies that
$$vol(S) = \sum_{x \in \Lambda} vol(S_x).$$
- Translate the pieces S_x into the fundamental parallelepiped by defining
$$\hat{S_x} = S_x - x.$$
Clearly $\hat{S_x} \subseteq P(B)$ and $vol(S_x)$.

Blichfeld's theorem (3)

- Furthermore,

$$\sum_{x \in \Lambda} vol(\hat{S}_x) = \sum_{x \in \Lambda} vol(S_x) = vol(S) > vol(P(B)).$$

Thus, there must exist $x \neq y \in \Lambda$ such that

$$\hat{S}_x \cap \hat{S}_y \neq \emptyset.$$

- Let $z \in \hat{S}_x \cap \hat{S}_y$. Then,

$$z + x \in S_x \subseteq S \text{ and } z + y \in S_y \subseteq S.$$

- Since $x, y \in \Lambda$,

$$(z + x) - (z + y) = x - y \in \Lambda.$$

Minkowski's convex body theorem (1)

Definition 17

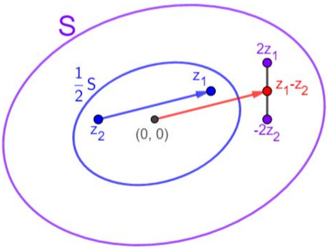
A subset $S \subseteq \mathbb{R}^n$ is called:

1. *centrally-symmetric* if for any $x \in S$ we also have $-x \in S$,
2. *convex* if for any $x, y \in S$ we also have $\mu x + (1-\mu)y \in S$ for all $\mu \in [0, 1]$.

Theorem 18 (Minkowski - convex body)

Let Λ be a full-rank lattice of rank n. Then, any centrally-symmetric convex set S with $vol(S) > 2^n \det(\Lambda)$ contains a non-zero lattice point.

Minkowski convex body example



Since $vol(S) > 4\det(\Lambda)$:

$vol(\frac{1}{2}S) = \frac{1}{4}vol(S) > \det(\Lambda)$.

Blichfeld's theorem implies the existence of a non-zero lattice point $z_1 - z_2$ which happens to be also in S.

Minkowski's convex body theorem (2)

Proof of theorem 18:

- Define
$$\hat{S} = \frac{1}{2}S = \{x \in \mathbb{R}^n : 2x \in S\}.$$
- Clearly
$$vol(\hat{S}) = 2^{-n} vol(S) > \det(\Lambda).$$
- Blichfeld's theorem implies that
$$\exists z_1 \neq z_2 \in \hat{S} \text{ such that } 0 \neq z_1 - z_2 \in \Lambda.$$
- By definition,
$$2z_1, 2z_2 \in S.$$
- Since S is centrally-symmetric,
$$-2z_2 \in S.$$
- Since S is convex,
$$\frac{2z_1 - 2z_2}{2} = z_1 - z_2 \in S.$$

Minkowski's first theorem (1)

Theorem 19 (Minkowski - 1)

For any full-rank lattice Λ of rank n,

$$\lambda_1(\Lambda) \leq \sqrt{n}(\det(\Lambda))^{1/n}.$$

$\sqrt{n}(\det(\Lambda))^{1/n}$ is called the *Minkowski bound*.

Minkowski's first theorem (2)

Proof of theorem 19:

- Consider the open sphere $B(0, \lambda_1(\Lambda))$ centered at 0 of radius $\lambda_1(\Lambda)$.
- By definition, $B(0, \lambda_1(\Lambda))$ is centrally-symmetric and convex but contains no non-zero lattice points.
- Minkowski's convex body theorem implies that

$$vol(B(0, \lambda_1(\Lambda))) \leq 2^n \det(\Lambda).$$

- Note that $B(0, \lambda_1(\Lambda))$ contains a cube of side length $\frac{2\lambda_1(\Lambda)}{\sqrt{n}}$ and so

$$\left(\frac{2\lambda_1(\Lambda)}{\sqrt{n}}\right)^n \leq vol(B(0, \lambda_1(\Lambda))).$$

- Thus,

$$\lambda_1(\Lambda) \leq \sqrt{n}(\det(\Lambda))^{1/n}.$$

Minkowski's first theorem (3)

Remarks 19

1. Using the fact that $vol(B(0, \lambda_1(\Lambda))) = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}(\lambda_1(\Lambda))^n$, one can obtain an upper bound for $\lambda_1(\Lambda)$ that is a lot tighter than $\sqrt{n}(\det(\Lambda))^{1/n}$.
2. $\lambda_1(\Lambda)$ can be very small compared to the Minkowski bound. Indeed, consider in dimension 2 the lattice given by $(1,0)^T$ and $(0,N)^T$ where $N \in \mathbb{N} \setminus \{0\}$. Then, the Minkovsky bound is $\sqrt{2}\sqrt{N}$ but $\lambda_1(\Lambda) = 1$.
3. $\lambda_1(\Lambda)$ can be very close to the Minkowski bound. Indeed, one can show, that in any dimension, there exists a lattice with shortest vector at least $c\sqrt{n}(\det(\Lambda))^{1/n}$ for some constant c.
4. It has been shown that $O(\sqrt{(n)}) \det(\Lambda)^{1/n}$ is the best upper bound one can possibly prove.
5. The term $(\det(\Lambda))^{1/n}$ makes sure that the expressions scale properly. Indeed, $\lambda_1(c\Lambda) = c\lambda_1(\Lambda)$ and $(\det(c\Lambda))^{1/n} = c(\det(\Lambda))^{1/n}$.

Minkowski's second theorem (1)

Theorem 20 (Minkowski - 2)

For any full-rank lattice Λ of rank n,

$$\left(\prod_{i=1}^{n} \lambda_i(\Lambda)\right)^{1/n} \leq \sqrt{n}(\det(\Lambda))^{1/n}.$$

Minkowski's second theorem (2)

Proof of theorem 20:

- Let $x_1, ..., x_n \in \Lambda$ be linearly independent vectors achieving the successive minima (i.e. $\|x_i\| = \lambda_i(\Lambda)$).
- Let $x_1^*, ..., x_n^*$ be their Gram-Schmidt orthogonalization.
- Consider the open ellipsoid T with axes $x_1^*, ..., x_n^*$ and lengths $\lambda_1(\Lambda), ..., \lambda_n(\Lambda)$,

$$T = \left\{ y \in \mathbb{R}^n : \sum_{i=1}^{n} \left(\frac{< y, x_i^* >}{\|x_i^*\| \lambda_i(\Lambda)} \right)^2 < 1 \right\}.$$

- Let $y \in \Lambda$ and let

$$k = \max\{k \in \{1, ..., n\} : \|y\| \geq \lambda_k(\Lambda)\}.$$

- Then,

$$y \in span(x_1^*, ..., x_k^*) = span(x_1, ..., x_k),$$

else $x_1, ..., x_k, y$ would be $k+1$ linearly independent vectors of length less than $\lambda_{k+1}(\Lambda)$.

Minkowski's second theorem (3)

- Thus,

$$\begin{aligned}\sum_{i=1}^{n}\left(\frac{< y, x_i^* >}{\|x_i^*\|\lambda_i(\Lambda)}\right)^2 &= \sum_{i=1}^{k}\left(\frac{< y, x_i^* >}{\|x_i^*\|\lambda_i(\Lambda)}\right)^2 \\ &\geq \frac{1}{(\lambda_k(\Lambda))^2}\sum_{i=1}^{k}\left(\frac{< y, x_i^* >}{\|x_i^*\|}\right)^2 \\ &= \frac{\|y\|^2}{(\lambda_k(\Lambda))^2} \\ &\geq 1.\end{aligned}$$

- Hence,

$$y \notin T.$$

Minkowski's second theorem (4)

- By Minkowski's convex body theorem,

$$vol(T) \geq 2^n \det(\Lambda).$$

- On the other hand, by the volume formula for ellipsoids,

$$vol(T) = \left(\prod_{i=1}^{n} \lambda_i(\Lambda)\right) vol(B(0,1)) \geq \left(\prod_{i=1}^{n} \lambda_i(\Lambda)\right) \left(\frac{2}{\sqrt{n}}\right)^n.$$

- Combining both bounds yields

$$\left(\prod_{i=1}^{n} \lambda_i(\Lambda)\right)^{1/n} \leq \sqrt{n}(\det(\Lambda))^{1/n}.$$

Minkowski's second theorem (5)

Remarks 21

1. Using the fact that $vol(B(0,1)) = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}$, one can obtain a better upper bound for the geometric mean $\left(\prod_{i=1}^{n} \lambda_i(\Lambda)\right)^{1/n}$.
2. The two previous results can easily be converted for any other norm.
3. The two previous results can be adapted to lattices of general rank.

Part VII:

Computational problems

Shortest vector problem

Search SVP

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find $v \in \mathcal{L}(B)$ such that $0 \neq \|v\| = \lambda_1(\mathcal{L}(B))$.

Optimization SVP

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find $\lambda_1(\mathcal{L}(B))$.

Decisional SVP

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a rational $r \in \mathbb{Q}$,
determine whether $\lambda_1(\mathcal{L}(B)) \leq r$ or not.

Surprisingly:

Search SVP $\Leftrightarrow$ Optimization SVP $\Leftrightarrow$ Decisional SVP

Approximate shortest vector problem

Let $\gamma \geq 1$.

Search SVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find $v \in \mathcal{L}(B)$ such that $0 \neq \|v\| \leq \gamma \lambda_1(\mathcal{L}(B))$.

Optimization SVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find d such that $d \leq \lambda_1(\mathcal{L}(B)) \leq \gamma d$.

Promise SVP$_\gamma$ or GapSVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a rational $r \in \mathbb{Q}$,
determine whether (B, r) belongs to the YES instance ($=\lambda_1(\mathcal{L}(B)) \leq r$) or to the NO instance ($\lambda_1(\mathcal{L}(B)) > \gamma r$).

Surprisingly:

$$\text{Search SVP}_\gamma \;\Rightarrow\; \text{Optimization SVP}_\gamma \;\Leftrightarrow\; \text{Promise SVP}_\gamma$$

Closest vector problem

Let $\gamma \geq 1$.

Search CVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a vector $t \in \mathbb{Z}^m$, find $v \in \mathcal{L}(B)$ such that $\|v - t\| \leq \gamma dist(t, \mathcal{L}(B))$.

Optimization CVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a vector $t \in \mathbb{Z}^m$, find d such that $d \leq dist(t, \mathcal{L}(B)) \leq \gamma d$.

Promise CVP$_\gamma$ or GapCVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$, a rational $r \in \mathbb{Q}$ and a vector $t \in \mathbb{Z}^m$, determine whether (B, r, t) belongs to the YES instance ($= dist(t, \mathcal{L}(B)) \leq r$) or to the NO instance ($= dist(t, \mathcal{L}(B)) > \gamma r$).

Miscellaneous lattice problems

SIVP

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find n linearly independent vectors $v_1, ..., v_n \in \mathcal{L}(B)$ such that $0 \neq \|v_i\| \leq \gamma\lambda_i(\mathcal{L}(B))$.

Bounded distance decoding

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a vector $t \in \mathbb{Z}^m$ such that $dist(t, \mathcal{L}(B)) < \frac{\lambda_1(\mathcal{L}(B))}{n}$ for a given $n \in \mathbb{N}$,
find $v \in \mathcal{L}(B)$ such that $\|v - t\| < \frac{\lambda_1(dist(t,\mathcal{L}(B)))}{n}$.

Covering radius problem

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find the largest distance from any vector to the lattice.

Remarks about lattice problems

Remarks 21

1. Many lattice problems are conjectured to be hard!
2. Finding the shortest vector is hard however, finding a short vector is manageable using different algorithms.
3. Many cryptographic schemes based on lattice problems seem to be secure and are even conjectured to be quantum secure.

References

References:

- Oded Regev's course notes "Lattices in Computer Science" (from 2004) from the Tel Aviv University that are accessible via the link: https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/
- Daniele Micciancio's course notes "Lattices Algorithms and Applications" (from 2010) from the University of California San Diego that are accessible via the link: http://cseweb.ucsd.edu/classes/wi10/cse206a/
- Chi's, Choi's, Kim's and Kim's lecture notes "Lattice Based Cryptography for Beginners" accessible via the link: https://eprint.iacr.org/2015/938.pdf
- Steven D. Galbraith's book "Mathematics of public key cryptography".