Basics of Lattice-Based Cryptography

Avijit Dutta

Institute for Advancing Intelligence, TCG CREST, India

June 27, 2025

What is Cryptology?

Cryptology is the science of secrecy.

Paradigms of Cryptography

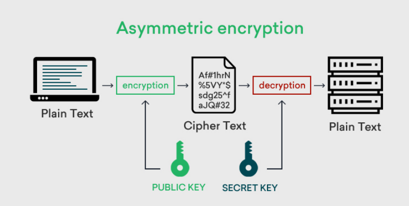


Figure: Public-key cryptography (RSA, El-Gamal, Diffie-Hellman)

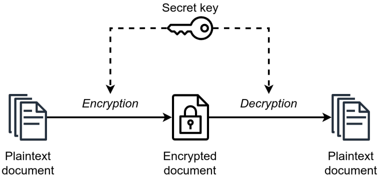


Figure: Symmetric-key cryptography (AES, DES, CBC, OCB)

Computational Assumption on the Security of Cryptographic Scheme

- Security of almost all cryptographic schemes are based on mathematical problems that are computationally difficult for classical computers to solve.
- For example, security of RSA is based on the hardness of factoring large integers.
- Security of OCB is based on the assumption that the underlying block cipher is secure.

Computational Assumption on the Security of Cryptographic Scheme

- Security of almost all cryptographic schemes are based on mathematical problems that are computationally difficult for classical computers to solve.
- For example, security of RSA is based on the hardness of factoring large integers.
- Security of OCB is based on the assumption that the underlying block cipher is secure.

Quantum computers can solve some of this mathematical hard problem efficiently

Quantum Algorithms

- **Shor's Algorithm:** Solve prime factors of a large integer in polynomial time.

Quantum Algorithms

- **Shor's Algorithm:** Solve prime factors of a large integer in polynomial time.
- **Grover's Search Algorithm:** Searching an unsorted list of N items, providing a quadratic speedup.

Quantum Algorithms

- **Shor's Algorithm:** Solve prime factors of a large integer in polynomial time.
- **Grover's Search Algorithm:** Searching an unsorted list of N items, providing a quadratic speedup.
- **Simon's Algorithm:** Period finding algorithm.

Quantum Algorithms

- **Shor's Algorithm:** Solve prime factors of a large integer in polynomial time.
- **Grover's Search Algorithm:** Searching an unsorted list of N items, providing a quadratic speedup.
- **Simon's Algorithm:** Period finding algorithm.

We require cryptographic schemes which are secure in the presence of quantum algorithms.

Quantum Algorithms

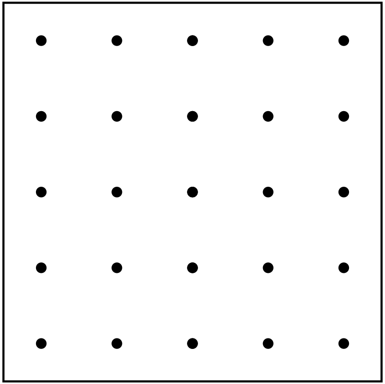
- **Shor's Algorithm:** Solve prime factors of a large integer in polynomial time.
- **Grover's Search Algorithm:** Searching an unsorted list of N items, providing a quadratic speedup.
- **Simon's Algorithm:** Period finding algorithm.

We require cryptographic schemes which are secure in the presence of quantum algorithms.

Lattice Based Cryptography is one of the possible candidates which are believed to be secure against quantum adversaries.

What is Lattice?

- A lattice can be thought of as any regularly spaced grid of points stretching out to infinity.



Definition of Lattice

Let $B = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k]$ be k linearly independent vectors in $\mathbb{R}^n$. Then,

$$\Lambda = \mathcal{L}(B) := \left\{ \sum_{i=1}^{k} x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}$$

is called lattice.

Definition of Lattice

Let $B = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k]$ be k linearly independent vectors in $\mathbb{R}^n$. Then,

$$\Lambda = \mathcal{L}(B) := \left\{ \sum_{i=1}^{k} x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}$$

is called lattice.

- B is called the *basis* of the lattice $\mathcal{L}(B)$.

Definition of Lattice

Let $B = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k]$ be k linearly independent vectors in $\mathbb{R}^n$. Then,

$$\Lambda = \mathcal{L}(B) := \left\{ \sum_{i=1}^{k} x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}$$

is called lattice.

- B is called the *basis* of the lattice $\mathcal{L}(B)$.
- (n, k) is called the (dimension, rank) of the lattice

Definition of Lattice

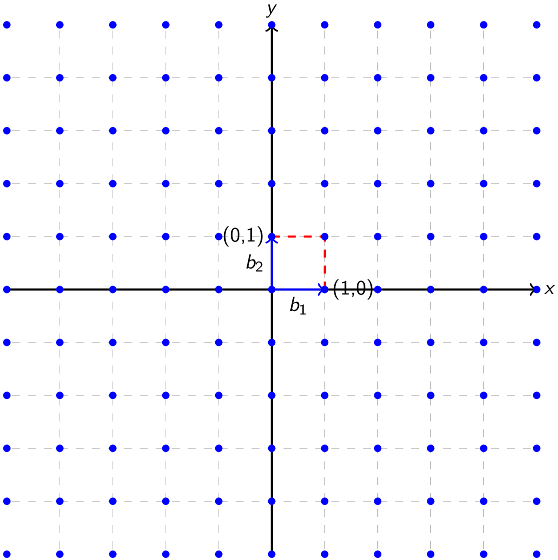
Let $B = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_k]$ be k linearly independent vectors in $\mathbb{R}^n$. Then,

$$\Lambda = \mathcal{L}(B) := \left\{ \sum_{i=1}^{k} x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}$$

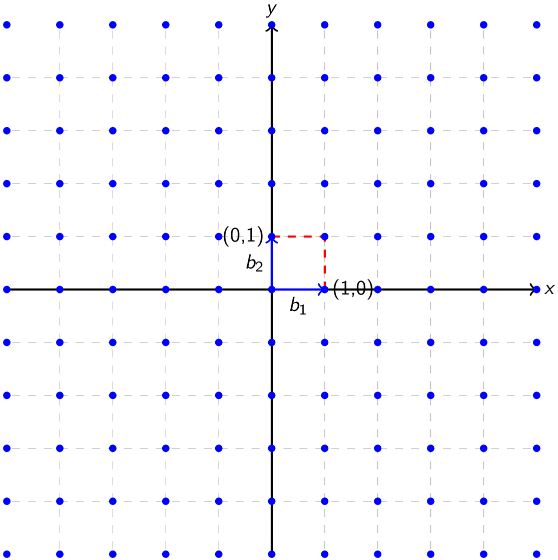
is called lattice.

- B is called the *basis* of the lattice $\mathcal{L}(B)$.
- (n, k) is called the (dimension, rank) of the lattice
- If $n = k$, then $\mathcal{L}(B)$ is called the *full rank lattice*.

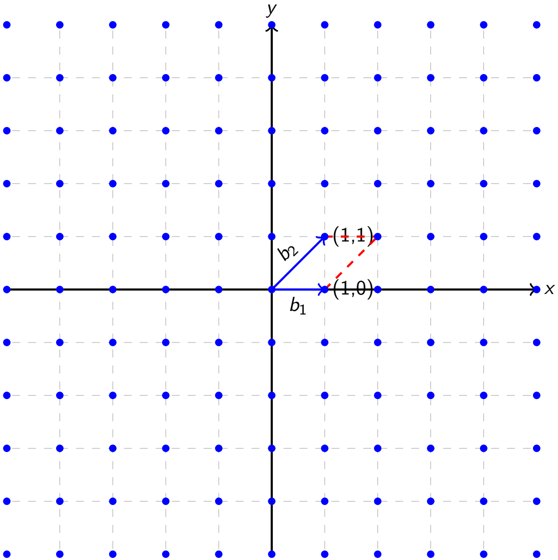
Example of Lattice



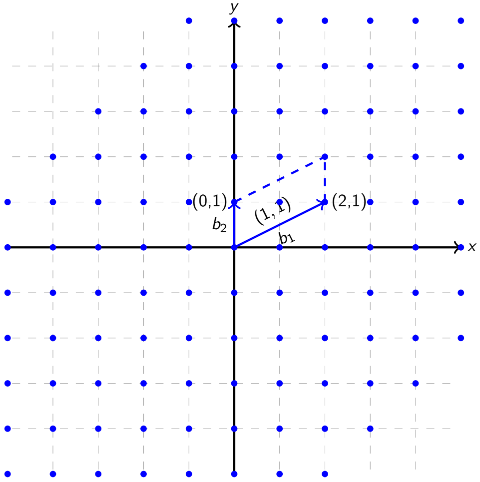
Is a Lattice Basis Unique ?



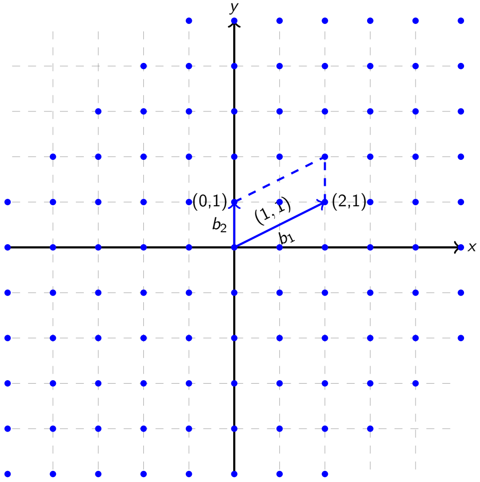
Another Basis of $\mathbb{Z}^2$



Does It Generate $\mathbb{Z}^2$?



Does It Generate $\mathbb{Z}^2$?



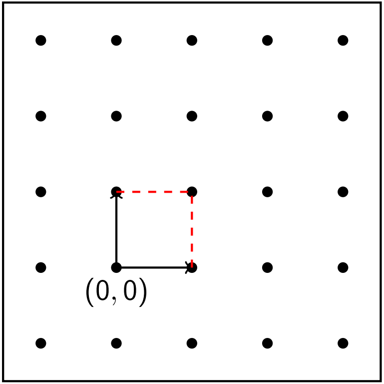
What is the criteria that two basis generate the same lattice ?

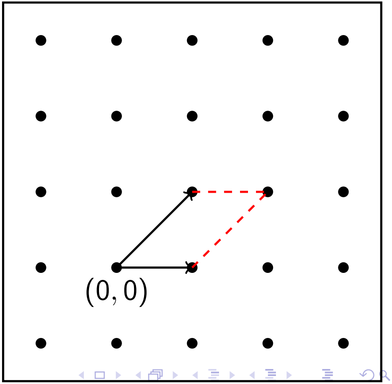
Transformation of Basis

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Transformation of Basis

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$



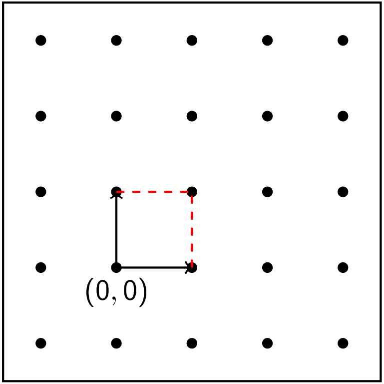


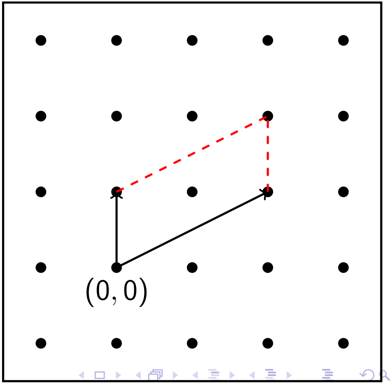
Transformation of Basis

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Transformation of Basis

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$





Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

- $\mathrm{GL}(n, \mathbb{Z})$ be the set of all invertible integer matrix of dimension $n \times n$

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

- $\mathrm{GL}(n, \mathbb{Z})$ be the set of all invertible integer matrix of dimension $n \times n$
- It is easy to see that $\mathrm{GL}(n, \mathbb{Z})$ is a group w.r.t matrix multiplication

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

- $\mathrm{GL}(n, \mathbb{Z})$ be the set of all invertible integer matrix of dimension $n \times n$
- It is easy to see that $\mathrm{GL}(n, \mathbb{Z})$ is a group w.r.t matrix multiplication

A matrix $U \in \mathbb{Z}^{n \times n}$ is called a unimodular matrix if $U \in \mathrm{GL}(n, \mathbb{Z})$

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Elementary Col operation leads to a unimodular matrix

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Elementary Col operation leads to a unimodular matrix

$$\text{(swap) } B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{unimodular}} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Elementary Col operation leads to a unimodular matrix

$$\text{(swap)}\ B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{unimodular}} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\text{(invert)}\ B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}}_{\text{unimodular}} = \begin{bmatrix} -2 & 1 \\ -1 & 0 \end{bmatrix}$$

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Two Basis Generate the Same Lattice

Let $B \in \mathbb{R}^{n\times k}, C \in \mathbb{R}^{n\times k}$. $B \equiv C$ iff $\exists U \in \mathrm{GL}(k, \mathbb{Z})$ such that $C = BU$.

Unimodular Matrix

- swap (i, j), i.e., $\vec{b}_i \leftrightarrow \vec{b}_j$
- invert (i), i.e., $\vec{b}_i \leftrightarrow -\vec{b}_i$
- add (i, j, c), i.e., $\vec{b}_i \leftarrow \vec{b}_i + c\vec{b}_j$ for some non-zero $c \in \mathbb{Z}$

Two Basis Generate the Same Lattice

Let $B \in \mathbb{R}^{n\times k}, C \in \mathbb{R}^{n\times k}$. $B \equiv C$ iff $\exists U \in \mathrm{GL}(k, \mathbb{Z})$ such that $C = BU$.

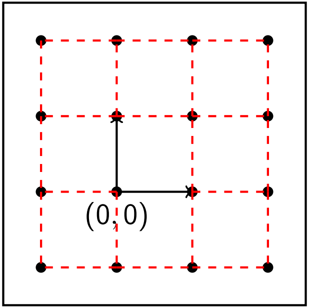
Fundamental Region and Fundamental Parallelepiped

Let $B \in \mathbb{R}^{n \times k}$ be a basis. We define fundamental parallelepiped corresponding to the lattice $\mathcal{L}(B)$ as $\mathcal{P}(B) := \{B.x : x \in \mathbb{R}^k, 0 \leq x_i < 1\}$.

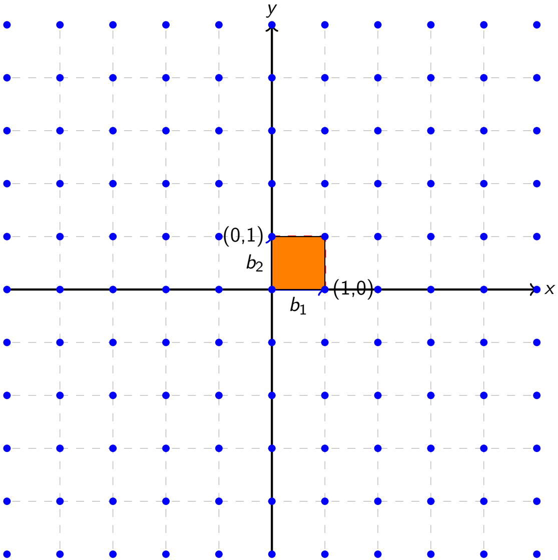
Fundamental Region and Fundamental Parallelepiped

Let $B \in \mathbb{R}^{n \times k}$ be a basis. We define fundamental parallelepiped corresponding to the lattice $\mathcal{L}(B)$ as $\mathcal{P}(B) := \{B.x : x \in \mathbb{R}^k, 0 \leq x_i < 1\}$.

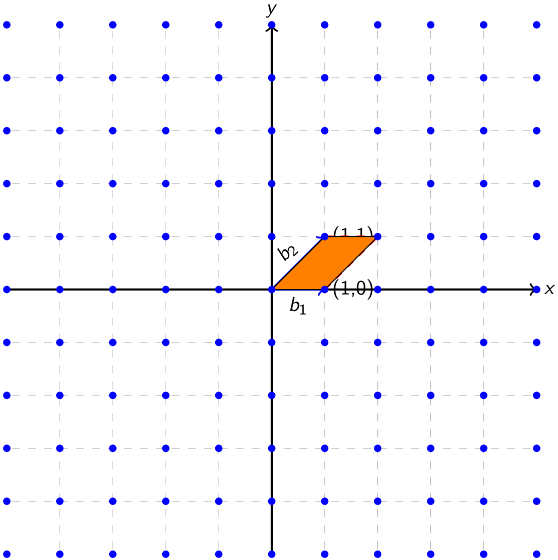
Property: Fundamental parallelepiped tiles the span of B.



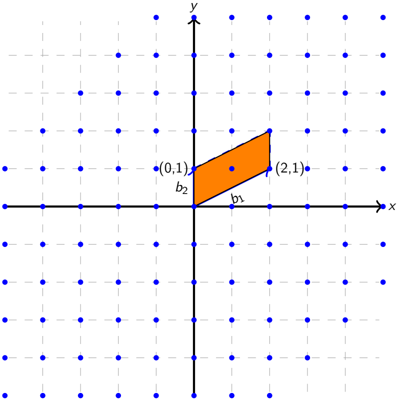
Examples of Fundamental Parallelepiped



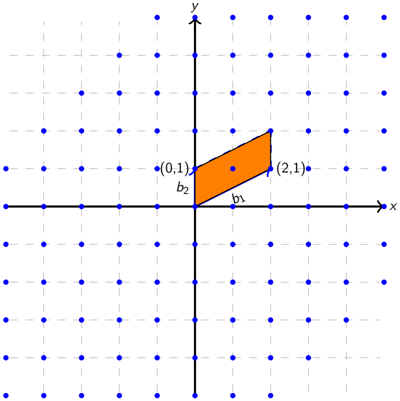
Fundamental Parallelepiped Changes with Basis



Fundamental Parallelepiped Changes with Basis



Fundamental Parallelepiped Changes with Basis



Given a lattice Λ and a set of linearly independent lattice vectors from Λ, when does it generate the same lattice ?

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Given a full rank lattice Λ and a set of n linearly independent lattice vectors $B = (b_1, b_2, \ldots, b_n) \in \Lambda$, $\mathcal{L}(B) = \Lambda$ if and only if $\Lambda \cap \mathcal{P}(B) = \{0\}$

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Given a full rank lattice Λ and a set of n linearly independent lattice vectors $B = (b_1, b_2, \ldots, b_n) \in \Lambda$, $\mathcal{L}(B) = \Lambda$ if and only if $\Lambda \cap \mathcal{P}(B) = \{0\}$

- (**only if:**) Λ is an integer linear combination and $\mathcal{P}(B)$ is $[0, 1)$ linear combination. Intersection must be a null vector

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Given a full rank lattice Λ and a set of n linearly independent lattice vectors $B = (b_1, b_2, \ldots, b_n) \in \Lambda$, $\mathcal{L}(B) = \Lambda$ if and only if $\Lambda \cap \mathcal{P}(B) = \{0\}$

- (**only if:**) Λ is an integer linear combination and $\mathcal{P}(B)$ is $[0, 1)$ linear combination. Intersection must be a null vector
- (**if:**) Let $v \in \Lambda$. $v = y_1\vec{x}_1 + y_2\vec{x}_2 + \ldots + y_n\vec{x}_n, y_i \in \mathbb{R}$.

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Given a full rank lattice Λ and a set of n linearly independent lattice vectors $B = (b_1, b_2, \ldots, b_n) \in \Lambda$, $\mathcal{L}(B) = \Lambda$ if and only if $\Lambda \cap \mathcal{P}(B) = \{0\}$

- (**only if:**) Λ is an integer linear combination and $\mathcal{P}(B)$ is $[0, 1)$ linear combination. Intersection must be a null vector
- (**if:**) Let $v \in \Lambda$. $v = y_1\vec{x}_1 + y_2\vec{x}_2 + \ldots + y_n\vec{x}_n, y_i \in \mathbb{R}$.
- $v' := (y_1 - \lfloor y_1 \rfloor)\vec{x}_1 + (y_2 - \lfloor y_2 \rfloor)\vec{x}_2 + (y_n - \lfloor y_n \rfloor)\vec{x}_n \in \Lambda$

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Given a full rank lattice Λ and a set of n linearly independent lattice vectors $B = (b_1, b_2, \ldots, b_n) \in \Lambda$, $\mathcal{L}(B) = \Lambda$ if and only if $\Lambda \cap \mathcal{P}(B) = \{0\}$

- (**only if:**) Λ is an integer linear combination and $\mathcal{P}(B)$ is $[0, 1)$ linear combination. Intersection must be a null vector
- (**if:**) Let $v \in \Lambda$. $v = y_1\vec{x}_1 + y_2\vec{x}_2 + \ldots + y_n\vec{x}_n, y_i \in \mathbb{R}$.
- $v' := (y_1 - \lfloor y_1 \rfloor)\vec{x}_1 + (y_2 - \lfloor y_2 \rfloor)\vec{x}_2 + (y_n - \lfloor y_n \rfloor)\vec{x}_n \in \Lambda$
- By hypothesis, $v' = 0 \Rightarrow (y_1 - \lfloor y_1 \rfloor)\vec{x}_1 + (y_2 - \lfloor y_2 \rfloor)\vec{x}_2 + (y_n - \lfloor y_n \rfloor)\vec{x}_n = 0$

Generator of Lattice

When do we say that a set of linearly independent lattice vectors is the generator of the lattice ?

Given a full rank lattice Λ and a set of n linearly independent lattice vectors $B = (b_1, b_2, \ldots, b_n) \in \Lambda$, $\mathcal{L}(B) = \Lambda$ if and only if $\Lambda \cap \mathcal{P}(B) = \{0\}$

- (**only if:**) Λ is an integer linear combination and $\mathcal{P}(B)$ is $[0, 1)$ linear combination. Intersection must be a null vector
- (**if:**) Let $v \in \Lambda$. $v = y_1\vec{x}_1 + y_2\vec{x}_2 + \ldots + y_n\vec{x}_n, y_i \in \mathbb{R}$.
- $v' := (y_1 - \lfloor y_1 \rfloor)\vec{x}_1 + (y_2 - \lfloor y_2 \rfloor)\vec{x}_2 + (y_n - \lfloor y_n \rfloor)\vec{x}_n \in \Lambda$
- By hypothesis, $v' = 0 \Rightarrow (y_1 - \lfloor y_1 \rfloor)\vec{x}_1 + (y_2 - \lfloor y_2 \rfloor)\vec{x}_2 + (y_n - \lfloor y_n \rfloor)\vec{x}_n = 0$
- $\because \vec{x}_1, \ldots, \vec{x}_n$ are linearly independent, $y_i - \lfloor y_i \rfloor = 0 \iff y_i = \lfloor y_i \rfloor$.

Determinant of a Lattice

- Determinant of a lattice $\Lambda = \mathcal{L}(B)$ is the volume of the fundamental parallelepiped $\mathcal{P}(B)$
- volume of the fundamental parallelepiped $\mathcal{P}(B)$ is $\sqrt{\det(B^T B)}$

Determinant of a Lattice

- Determinant of a lattice $\Lambda = \mathcal{L}(B)$ is the volume of the fundamental parallelepiped $\mathcal{P}(B)$
- volume of the fundamental parallelepiped $\mathcal{P}(B)$ is $\sqrt{\det(B^T B)}$

Lemma

If $B \equiv C$, then $\text{vol}(\mathcal{P}(B)) = \text{vol}(\mathcal{P}(C))$

Determinant of a Lattice

- Determinant of a lattice $\Lambda = \mathcal{L}(B)$ is the volume of the fundamental parallelepiped $\mathcal{P}(B)$
- volume of the fundamental parallelepiped $\mathcal{P}(B)$ is $\sqrt{\det(B^T B)}$

Lemma

If $B \equiv C$, then $\text{vol}(\mathcal{P}(B)) = \text{vol}(\mathcal{P}(C))$

- Algebraic proof is routine calculation
- volume of an object remains unaffected with respect to elementary column operation

Determinant of a Lattice

- Determinant of a lattice $\Lambda = \mathcal{L}(B)$ is the volume of the fundamental parallelepiped $\mathcal{P}(B)$
- volume of the fundamental parallelepiped $\mathcal{P}(B)$ is $\sqrt{\det(B^T B)}$

Lemma

If $B \equiv C$, then $\text{vol}(\mathcal{P}(B)) = \text{vol}(\mathcal{P}(C))$

- Algebraic proof is routine calculation
- volume of an object remains unaffected with respect to elementary column operation

Note: $\det(\Lambda) \propto \frac{1}{\text{density}(\Lambda)}$.

Gram Schmidt Orthogonalization

- Let $B = b_1, b_2, \ldots, b_n$ that generates a finite dimensional vector space V.

Gram Schmidt Orthogonalization

- Let $B = b_1, b_2, \ldots, b_n$ that generates a finite dimensional vector space V.
- We define $\pi_i : \mathbb{R}^n \rightarrow \text{span}(b_1, \ldots, b_{i-1})$ defined as

$$\pi_i(x) = x - \sum_{j=1}^{i-1} \frac{\langle x, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*$$

- Note that $\pi_i(x) = x \perp \text{span}(b_1, b_2, \ldots, b_{i-1})$.

Gram Schmidt Orthogonalization

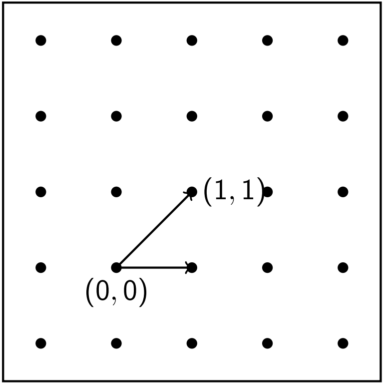
- Let $B = b_1, b_2, \ldots, b_n$ that generates a finite dimensional vector space V.
- We define $\pi_i : \mathbb{R}^n \rightarrow \text{span}(b_1, \ldots, b_{i-1})$ defined as

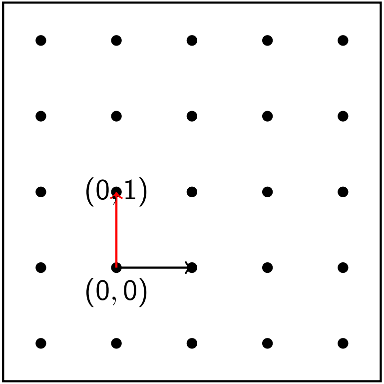
$$\pi_i(x) = x - \sum_{j=1}^{i-1} \frac{\langle x, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*$$

- Note that $\pi_i(x) = x \perp \text{span}(b_1, b_2, \ldots, b_{i-1})$.

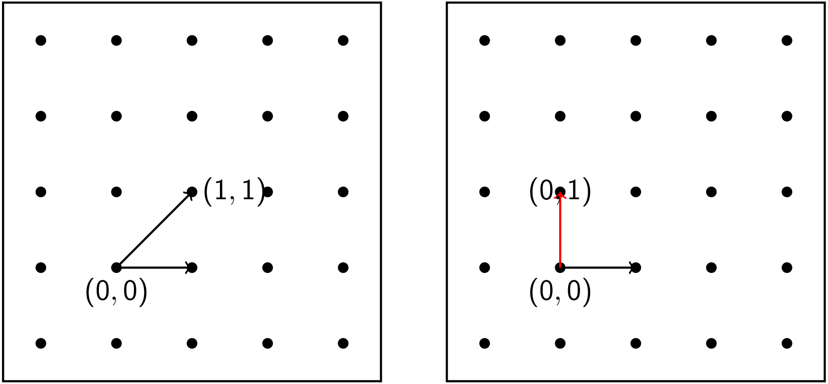
The GSO of a sequence of vectors $B = (b_1, b_2, \ldots, b_n)$ is the sequence $B^* = (\pi_1(b_1), \pi_2(b_2), \ldots, \pi_n(b_n))$.

Example of GSO



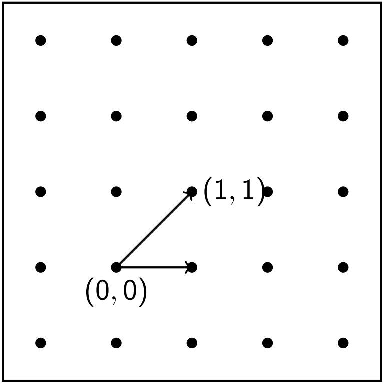


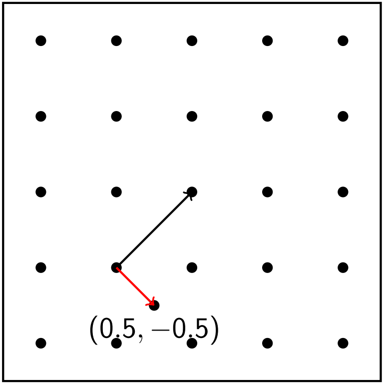
Example of GSO



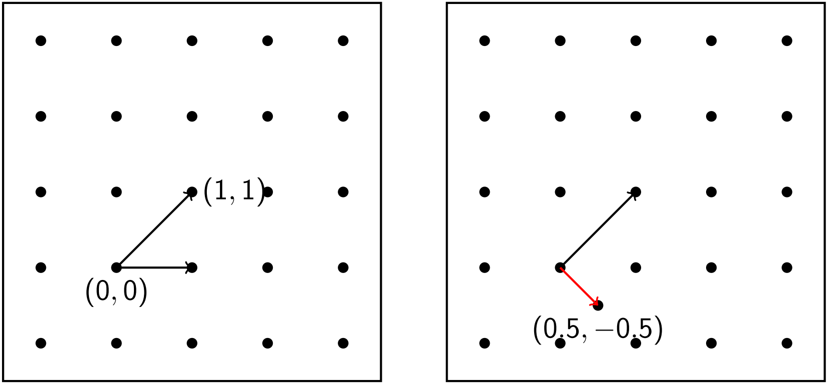
Both the basis generate the same lattice

Example of GSO



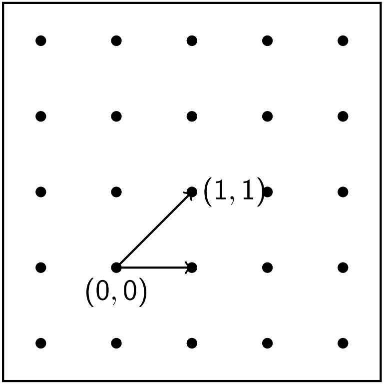


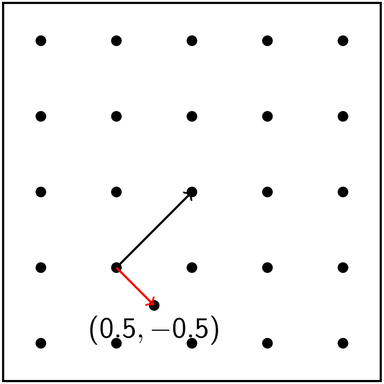
Example of GSO



- These two basis do not generate the same lattice.
- However they span the same vector space $\mathbb{R}^2$

Example of GSO





- These two basis do not generate the same lattice.
- However they span the same vector space $\mathbb{R}^2$

In general, $\mathcal{L}(B) \neq \mathcal{L}(B^*)$

Determinant of a Lattice and Gram-Schmidt Vectors

Lemma

Ler B be a basis and B^* be its GSO. Then, $\text{vol}(\mathcal{P}(B)) = \prod_{i=1}^{n} \|b_i^*\|$

Determinant of a Lattice and Gram-Schmidt Vectors

Lemma

Ler B be a basis and B^* be its GSO. Then, $\mathrm{vol}(\mathcal{P}(B)) = \prod_{i=1}^{n} \|b_i^*\|$

- Consider $n = 2$. Let $B = (b_1, b_2)$.
- $\mathcal{P}(B)$ is a parallelogram with sides b_1 and b_2
- The area of the parallelogram is $\|b_1\| \times \|b_2^*\|$
- Let it be true for dimension $n - 1$
- For n-dimension, $\mathrm{vol}(\mathcal{P}(B)) =$ vol of $n - 1$ dimensional fundamental parallelopiped $\times \|b_n^*\|$.

Determinant of a Lattice and Gram-Schmidt Vectors

Lemma

Ler B be a basis and B^* be its GSO. Then, $\text{vol}(\mathcal{P}(B)) = \prod_{i=1}^{n} \|b_i^*\|$

- Consider $n = 2$. Let $B = (b_1, b_2)$.
- $\mathcal{P}(B)$ is a parallelogram with sides b_1 and b_2
- The area of the parallelogram is $\|b_1\| \times \|b_2^*\|$
- Let it be true for dimension $n - 1$
- For n-dimension, $\text{vol}(\mathcal{P}(B)) =$ vol of $n - 1$ dimensional fundamental parallelopiped $\times \|b_n^*\|$.

Since $\|b_i^*\| \leq \|b_i\|$, we have $\text{vol}(\mathcal{P}(B)) \leq \prod_i \|b_i\|$.

Minimum Distance of a Lattice

For any lattice Λ, the minimum distance of Λ is the smallest distance between any two lattice points, i.e.,

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

Minimum Distance of a Lattice

For any lattice Λ, the minimum distance of Λ is the smallest distance between any two lattice points, i.e.,

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

Since, Λ is a discrete additive subgroup of $\mathbb{R}^n$, we can alternatively defined it the minimum norm of a non-zero lattice vector, i.e.,

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

Minimum Distance of a Lattice

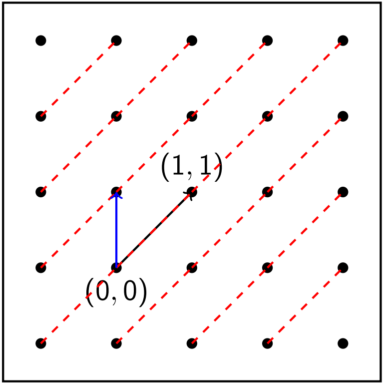
Lemma

For every lattice basis B and its Gram-Schmidt orthogonalization B^*, $\lambda_1(\mathcal{L}(B)) \geq \min_i \|\vec{b}_i^*\|$.

Minimum Distance of a Lattice

Lemma

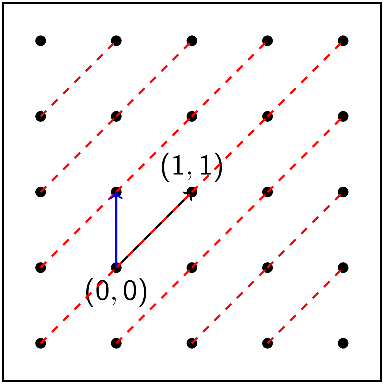
For every lattice basis B and its Gram-Schmidt orthogonalization B^*, $\lambda_1(\mathcal{L}(B)) \geq \min_i \|\vec{b}_i^*\|$.

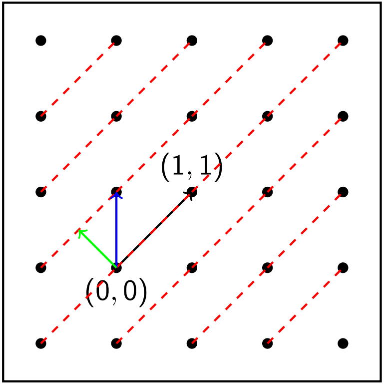


Minimum Distance of a Lattice

Lemma

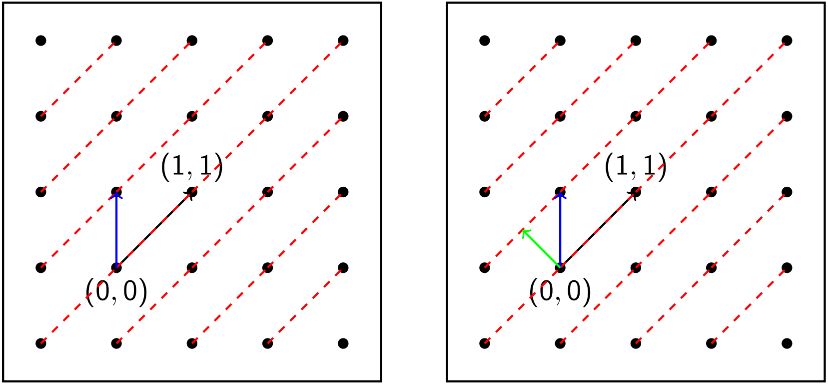
For every lattice basis B and its Gram-Schmidt orthogonalization B^*, $\lambda_1(\mathcal{L}(B)) \geq \min_i \|\vec{b}_i^*\|$.





Lemma

For every lattice basis B and its Gram-Schmidt orthogonalization B^*, $\lambda_1(\mathcal{L}(B)) \geq \min_i \|\vec{b}_i^*\|$.



Any discrete subgroup of $\mathbb{R}^n$ is a lattice

Minimum Distance of a Lattice

Lemma

For every lattice basis B, there is always a non-zero lattice vector $x \in \mathcal{L}(B)$ such that $\|x\| = \lambda_1(\mathcal{L}(B))$.

Minimum Distance of a Lattice

Lemma

For every lattice basis B, there is always a non-zero lattice vector $x \in \mathcal{L}(B)$ such that $\|x\| = \lambda_1(\mathcal{L}(B))$.

- A ball centered at 0 and of some radius k contains only finitely many balls of radius λ_1 centered at lattice points within the ball.

Minimum Distance of a Lattice

Lemma

For every lattice basis B, there is always a non-zero lattice vector $x \in \mathcal{L}(B)$ such that $\|x\| = \lambda_1(\mathcal{L}(B))$.

- A ball centered at 0 and of some radius k contains only finitely many balls of radius λ_1 centered at lattice points within the ball.
- A consequence is that the ball centered at 0 and radius k will contain finitely many lattice points.

Minimum Distance of a Lattice

Lemma

For every lattice basis B, there is always a non-zero lattice vector $x \in \mathcal{L}(B)$ such that $\|x\| = \lambda_1(\mathcal{L}(B))$.

- A ball centered at 0 and of some radius k contains only finitely many balls of radius λ_1 centered at lattice points within the ball.
- A consequence is that the ball centered at 0 and radius k will contain finitely many lattice points.
- Consider a closed ball $B(0, 2\lambda_1)$. This contains finitely many lattice points. Then by definition of λ_1 , there is at least one lattice point of length λ_1.

Minkowski's Bound on λ_1

For any n-dimensional lattice Λ, $\lambda_1(\Lambda) \leq \sqrt{n}\det(\Lambda)^{1/n}$

Minkowski's Bound on λ_1

For any n-dimensional lattice Λ, $\lambda_1(\Lambda) \leq \sqrt{n}\det(\Lambda)^{1/n}$

- **Blitchfeldt Theorem:** $\text{vol}(S) > \det(\mathcal{L}(B)) \Rightarrow \exists z_1, z_2 \in S$ such that $z_1 - z_2 \in \mathcal{L}(B)$.
- **Convex Body Theorem:** If S is a centrally symmetric and convex body of $\text{vol}(S) > 2^n \det(\Lambda)$, then S contains a non-zero lattice point.

Minkowski's Bound on λ_1

For any n-dimensional lattice Λ, $\lambda_1(\Lambda) \leq \sqrt{n}\det(\Lambda)^{1/n}$

- **Blitchfeldt Theorem:** $\text{vol}(S) > \det(\mathcal{L}(B))) \Rightarrow \exists z_1, z_2 \in S$ such that $z_1 - z_2 \in \mathcal{L}(B)$.
- **Convex Body Theorem:** If S is a centrally symmetric and convex body of $\text{vol}(S) > 2^n\det(\Lambda)$, then S contains a non-zero lattice point.

(**Tightness of the Bound:**) Let D be a large integer.

$$B = \begin{bmatrix} 1 & 0 \\ 0 & D \end{bmatrix}$$

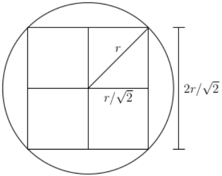
Note that, $\lambda_1(\mathcal{L}(B)) = 1$ but, the result says $\lambda_1(\mathcal{L}(B)) \leq \sqrt{2D}$

Proof of Minkowski's Bound

Volume of an n-dimensional ball of radius r is $\left(\frac{2r}{\sqrt{n}}\right)^n$

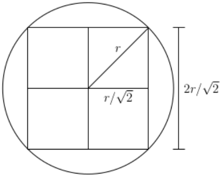
Proof of Minkowski's Bound

Volume of an n-dimensional ball of radius r is $\left(\frac{2r}{\sqrt{n}}\right)^n$



Proof of Minkowski's Bound

Volume of an n-dimensional ball of radius r is $\left(\frac{2r}{\sqrt{n}}\right)^n$



- $\text{vol}(B(0, \lambda_1)) \geq \left(\frac{2\lambda_1}{\sqrt{n}}\right)^n$
- $\text{vol}(B(0, \lambda_1)) \leq 2^n \det(\mathcal{L}(B))$ – (MCB Theorem)

Proof of Minkowski's Convex Body Theorem

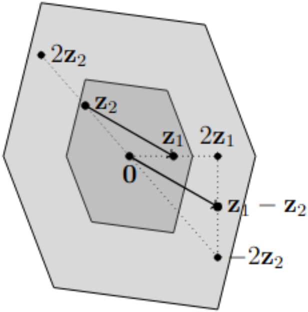
Minkowski's Convex Body Theorem

Let Λ be a full-rank lattice of dimension n. If $S \subseteq \mathbb{R}^n$ is a centrally symmetric and convex body of volume $\text{vol}(S) > 2^n \det(\Lambda)$, then S contains a non-zero lattice point.

Proof of Minkowski's Convex Body Theorem

Minkowski's Convex Body Theorem

Let Λ be a full-rank lattice of dimension n. If $S \subseteq \mathbb{R}^n$ is a centrally symmetric and convex body of volume $\text{vol}(S) > 2^n \det(\Lambda)$, then S contains a non-zero lattice point.



Proof of Blitchfeldt Theorem

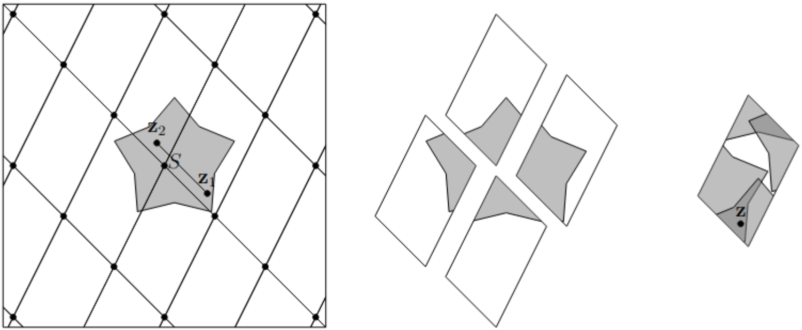
Blitchfeldt Theorem

Let B be a basis and Λ be an n-dimensional full rank lattice. Let $S \subseteq \text{span}(\Lambda)$ be a measureable set such that $\text{vol}(S) > \det(\Lambda)$. Then, there exists two points z_1, z_2 such that $z_1 - z_2 \in \Lambda$.

Proof of Blitchfeldt Theorem

Blitchfeldt Theorem

Let B be a basis and Λ be an n-dimensional full rank lattice. Let $S \subseteq \text{span}(\Lambda)$ be a measureable set such that $\text{vol}(S) > \det(\Lambda)$. Then, there exists two points z_1, z_2 such that $z_1 - z_2 \in \Lambda$.

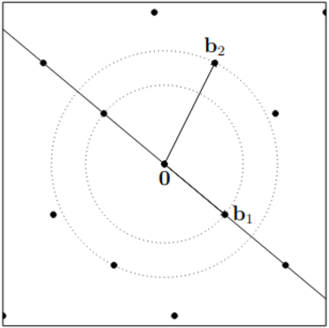


Successive Minima of Lattice

For an n-dimensional lattice Λ and an integer $k \leq n$, $\lambda_k(\Lambda)$ be the smallest $r > 0$ such that Λ contains at least k linearly independent vectors of length at most r

Successive Minima of Lattice

For an n-dimensional lattice Λ and an integer $k \leq n$, $\lambda_k(\Lambda)$ be the smallest $r > 0$ such that Λ contains at least k linearly independent vectors of length at most r



Successive Minima of Lattice

For an n-dimensional lattice Λ and an integer $k \leq n$, $\lambda_k(\Lambda)$ be the smallest $r > 0$ such that Λ contains at least k linearly independent vectors of length at most r

Minkowski's Second Theorem

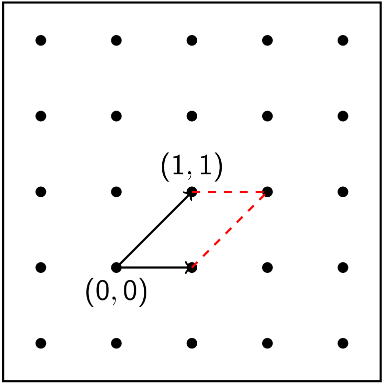
For an n-dimensional lattice Λ, $(\prod_i(\lambda_i))^{1/n} \leq \sqrt{\gamma_n}(\det(\Lambda))^{1/n}$, where γ_n is the Hermite constant.

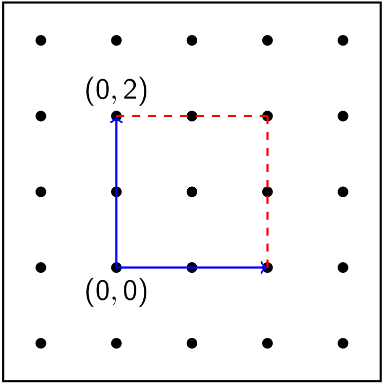
Sublattice

Defn: Let Λ be a lattice of dimension n. We call Λ' to be a sublattice of Λ if (a) $\Lambda' \subseteq \Lambda$ and (b) Λ' is itself a lattice

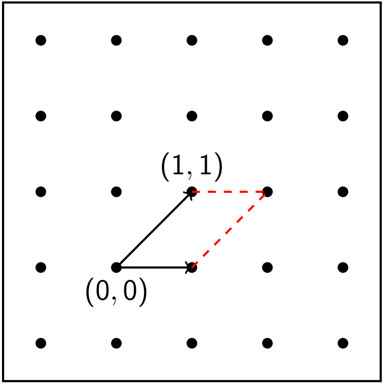
Sublattice

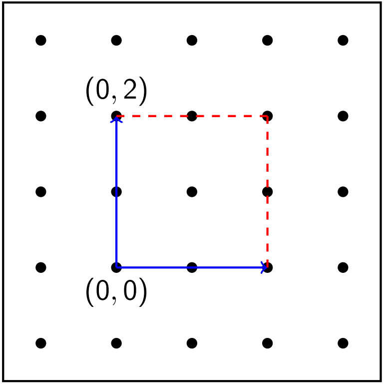
Defn: Let Λ be a lattice of dimension n. We call Λ' to be a sublattice of Λ if (a) $\Lambda' \subseteq \Lambda$ and (b) Λ' is itself a lattice





Sublattice





$$B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = B \cdot \begin{bmatrix} 2 & -2 \\ 0 & 2 \end{bmatrix}$$

Sublattice

Theorem

Let B and C be two basis. Then $\mathcal{L}(B) \subseteq \mathcal{L}(C)$ if and only if there exists an integer matrix U such that $B = CU$

Sublattice

Theorem

Let B and C be two basis. Then $\mathcal{L}(B) \subseteq \mathcal{L}(C)$ if and only if there exists an integer matrix U such that $B = CU$

- let $v \in \mathcal{L}(B)$. v can be written as integer linear combination of B vectors
- Since $B = CU$, v can also be expressed as an integer linear combination of C vectors. Thus, $v \in \mathcal{L}(C)$
- On the other hand, each B vectors are expressed as an integer linear combination of C vectors. Thus, each B vectors $\in \mathcal{L}(C)$. Thus, any $v \in \mathcal{L}(B) \Rightarrow v \in \mathcal{L}(C)$.

Sublattice

Theorem

Let B and C be two basis. Then $\mathcal{L}(B) \subseteq \mathcal{L}(C)$ if and only if there exists an integer matrix U such that $B = CU$

- let $v \in \mathcal{L}(B)$. v can be written as integer linear combination of B vectors
- Since $B = CU$, v can also be expressed as an integer linear combination of C vectors. Thus, $v \in \mathcal{L}(C)$
- On the other hand, each B vectors are expressed as an integer linear combination of C vectors. Thus, each B vectors $\in \mathcal{L}(C)$. Thus, any $v \in \mathcal{L}(B) \Rightarrow v \in \mathcal{L}(C)$.

Note that, $\frac{\det(\mathcal{L}(B))}{\det(\mathcal{L}(C))}$ should be an integer.

Group Theoretic View of Lattice and Sublattice

Defn: An n-dimensional Lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$

Discrete means there exists an $\epsilon > 0$ such that for all $x \neq y \in \Lambda$, $\|x - y\| > \epsilon$

Group Theoretic View of Lattice and Sublattice

Defn: An n-dimensional Lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$

Discrete means there exists an $\epsilon > 0$ such that for all $x \neq y \in \Lambda$, $\|x - y\| > \epsilon$

Since Λ is a additive subgroup, an alternative characterization of discrete is as follows:

$$\exists \epsilon > 0 \text{ such that } \forall x \in \Lambda \setminus \{0\}, \|x\| > \epsilon.$$

Group Theoretic View of Lattice and Sublattice

Defn: An n-dimensional Lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$

Discrete means there exists an $\epsilon > 0$ such that for all $x \neq y \in \Lambda$, $\|x - y\| > \epsilon$

Since Λ is a additive subgroup, an alternative characterization of discrete is as follows:

$$\exists \epsilon > 0 \text{ such that } \forall x \in \Lambda \setminus \{0\}, \|x\| > \epsilon.$$

It can be shown that the two definitions of lattice are equivalent

Group Theoretic View of Lattice and Sublattice

Defn: A sublattice $\Lambda' \subseteq \Lambda$ is a normal subgroup of Λ

Group Theoretic View of Lattice and Sublattice

Defn: A sublattice $\Lambda' \subseteq \Lambda$ is a normal subgroup of Λ

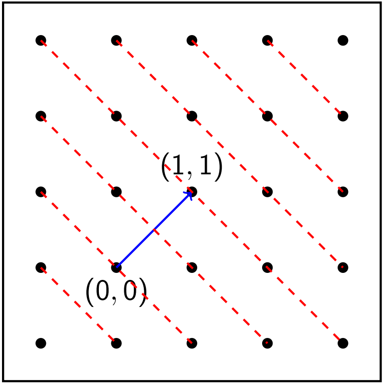
- Define an equivalence relation $\equiv_{\Lambda'}$ over Λ as $x \equiv_{\Lambda'} y$ iff $x - y \in \Lambda'$
- For $x, x' \in [x]$ and $y, y' \in [y]$, $[x] + [y] = [x + y]$ which is defined as $x + x' \equiv_{\Lambda'} y + y'$
- The collection of equivalence classes along with the operation '$+$' constitute a group, called **quotient group**, denoted as Λ/Λ'
- Each equivalence class $[x]$ is a set $x + \Lambda'$ which is known as a **coset**, where $x + \Lambda = \{v \in \Lambda : v - x \in \Lambda'\}$
- Note that $\Lambda = \bigcup_{x \in \Lambda/\Lambda'} x + \Lambda'$

Dual Lattice

Defn: A dual lattice $\widehat{\Lambda}$ of a given lattice Λ is the set of all vectors $x \in \text{span}(\Lambda)$ such that $\langle x, y \rangle$ is an integer for all $y \in \Lambda$

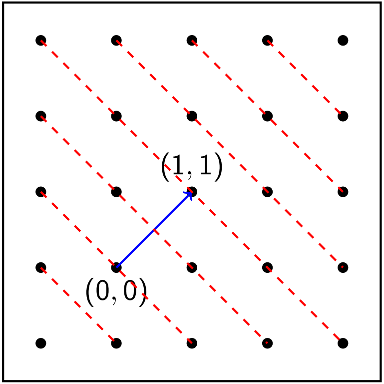
Dual Lattice

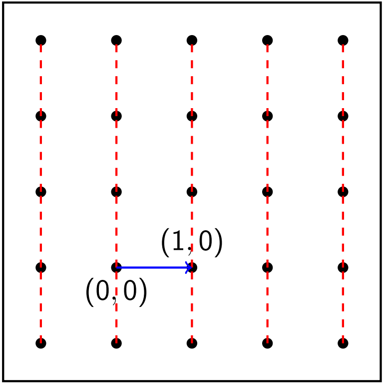
Defn: A dual lattice $\widehat{\Lambda}$ of a given lattice Λ is the set of all vectors $x \in \text{span}(\Lambda)$ such that $\langle x, y \rangle$ is an integer for all $y \in \Lambda$



Dual Lattice

Defn: A dual lattice $\widehat{\Lambda}$ of a given lattice Λ is the set of all vectors $x \in \text{span}(\Lambda)$ such that $\langle x, y \rangle$ is an integer for all $y \in \Lambda$





Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^\mathsf{T}B)^{-1}$

Properties of Dual Lattice

> The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathsf{T}}B)^{-1}$

- Let $G = B^{\mathsf{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathsf{T}}B^{-1}y) \in \mathrm{span}(B)$

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.
- Consider $\langle Dy, Bx \rangle \in \mathbb{Z}$.

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.
- Consider $\langle Dy, Bx \rangle \in \mathbb{Z}$.

$$\mathcal{L}(D) \subseteq \widehat{\mathcal{L}(B)}$$

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.
- Consider $\langle Dy, Bx \rangle \in \mathbb{Z}$.

$$\mathcal{L}(D) \subseteq \widehat{\mathcal{L}(B)}$$

- Let $v \in \widehat{\mathcal{L}(B)}$.

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.
- Consider $\langle Dy, Bx\rangle \in \mathbb{Z}$.

$$\mathcal{L}(D) \subseteq \widehat{\mathcal{L}(B)}$$

- Let $v \in \widehat{\mathcal{L}(B)}$.
- By definition, $v \in \mathrm{span}(B)$ and $B^{\mathrm{T}}v \in \mathbb{Z}^k$.

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.
- Consider $\langle Dy, Bx \rangle \in \mathbb{Z}$.

$$\mathcal{L}(D) \subseteq \widehat{\mathcal{L}(B)}$$

- Let $v \in \widehat{\mathcal{L}(B)}$.
- By definition, $v \in \mathrm{span}(B)$ and $B^{\mathrm{T}}v \in \mathbb{Z}^k$.
- Therefore, $v = Bw = B(B^{\mathrm{T}}B)^{-1}(B^{\mathrm{T}}B)w = D(B^{\mathrm{T}}v) \in \mathcal{L}(D)$

Properties of Dual Lattice

The dual of a lattice with basis B is a lattice with basis $D = B(B^{\mathrm{T}}B)^{-1}$

- Let $G = B^{\mathrm{T}}B$.
- Consider a vector $Dy \in \mathcal{L}(D)$
- Note that, $Dy = B(B^{\mathrm{T}}B^{-1}y) \in \mathrm{span}(B)$
- Let $Bx \in \mathcal{L}(B)$ be any arbitrary vector.
- Consider $\langle Dy, Bx \rangle \in \mathbb{Z}$.

$$\mathcal{L}(D) \subseteq \widehat{\mathcal{L}(B)}$$

- Let $v \in \widehat{\mathcal{L}(B)}$.
- By definition, $v \in \mathrm{span}(B)$ and $B^{\mathrm{T}}v \in \mathbb{Z}^k$.
- Therefore, $v = Bw = B(B^{\mathrm{T}}B)^{-1}(B^{\mathrm{T}}B)w = D(B^{\mathrm{T}}v) \in \mathcal{L}(D)$

$$\widehat{\mathcal{L}(B)} \subseteq \mathcal{L}(D)$$

Properties of Dual Lattice

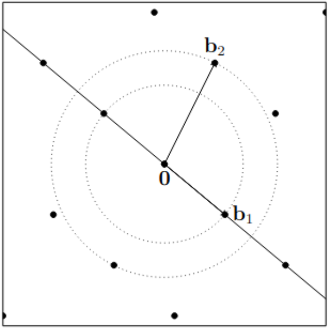
- Dual of the dual lattice is the original lattice
- D is the dual basis of B if and only if the $\text{span}(B) = \text{span}(D)$ and $B^T D = D^T B = I$
- Determinant of a dual lattice is the inverse of the determinant of its original lattice

Properties of Dual Lattice

- Dual of the dual lattice is the original lattice
- D is the dual basis of B if and only if the $\text{span}(B) = \text{span}(D)$ and $B^{\mathtt{T}}D = D^{\mathtt{T}}B = I$
- Determinant of a dual lattice is the inverse of the determinant of its original lattice

You can prove all the above properties at home!

Transference Theorem Related to Successive Minima



Goal: Consider Λ with successive minima $\lambda_1, \ldots, \lambda_n$ and $\widehat{\Lambda}$ be the dual lattice of Λ with successive minima $\widehat{\lambda_1}, \ldots, \widehat{\lambda_n}$. Can we transfer knowledge from $\lambda_1, \ldots, \lambda_n$ to $\widehat{\lambda_1}, \ldots, \widehat{\lambda_n}$?

What can we say about λ_1

- By Minkowski's Theorem, we have

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

What can we say about λ_1

- By Minkowski's Theorem, we have

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

- Similarly, we have

$$\widehat{\lambda_1} \le \sqrt{n} \cdot \det(\widehat{\Lambda})^{1/n} = \sqrt{n} \cdot \det(\widehat{\Lambda})^{-1/n}.$$

What can we say about λ_1

- By Minkowski's Theorem, we have

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

- Similarly, we have

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

- Therefore, we have

$$\lambda_1 \cdot \widehat{\lambda_1} \leq n.$$

What can we say about λ_1

- By Minkowski's Theorem, we have

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

- Similarly, we have

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

- Therefore, we have

$$\lambda_1 \cdot \widehat{\lambda_1} \leq n.$$

- **Consequence:** if λ_1 is large then $\widehat{\lambda_1}$ is small.

What can we say about λ_1

- By Minkowski's Theorem, we have

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

- Similarly, we have

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

- Therefore, we have

$$\lambda_1 \cdot \widehat{\lambda_1} \leq n.$$

- **Consequence:** if λ_1 is large then $\widehat{\lambda_1}$ is small.

Remark

Using the stronger version of Minkowski's Theorem, one has

$$\lambda_1 \cdot \widehat{\lambda_1} \leq \gamma_n.$$

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$
- Let $x_1, x_2, \ldots, x_n \in \widehat{\Lambda}$ such that $\|x_n\| = \widehat{\lambda_n}$ and $\|x_i\| \leq \|x_n\|$

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$
- Let $x_1, x_2, \ldots, x_n \in \widehat{\Lambda}$ such that $\|x_n\| = \widehat{\lambda_n}$ and $\|x_i\| \leq \|x_n\|$
- **Observation:** $\exists j$ such that $\langle v, x_j \rangle \in \mathbb{Z} \setminus 0$. (**Why ?**)

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$
- Let $x_1, x_2, \ldots, x_n \in \widehat{\Lambda}$ such that $\|x_n\| = \widehat{\lambda_n}$ and $\|x_i\| \leq \|x_n\|$
- **Observation:** $\exists j$ such that $\langle v, x_j \rangle \in \mathbb{Z} \setminus 0$. (**Why ?**)

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$
- Let $x_1, x_2, \ldots, x_n \in \widehat{\Lambda}$ such that $\|x_n\| = \widehat{\lambda_n}$ and $\|x_i\| \leq \|x_n\|$
- **Observation:** $\exists j$ such that $\langle v, x_j \rangle \in \mathbb{Z} \setminus 0$. (**Why ?**)

$$1 \leq |\langle v, x_j \rangle| \leq \|v\| \|x_j\| \leq \lambda_1 \cdot \widehat{\lambda_n}$$

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$
- Let $x_1, x_2, \ldots, x_n \in \widehat{\Lambda}$ such that $\|x_n\| = \widehat{\lambda_n}$ and $\|x_i\| \leq \|x_n\|$
- **Observation:** $\exists j$ such that $\langle v, x_j \rangle \in \mathbb{Z} \setminus 0$. (**Why ?**)

$$1 \leq |\langle v, x_j \rangle| \leq \|v\| \|x_j\| \leq \lambda_1 \cdot \widehat{\lambda_n}$$

More generally, $\forall 1 \leq k \leq n$

$$1 \leq \lambda_k \cdot \widehat{\lambda_{n-k+1}} \leq n.$$

Another Transference Theorem

Transference Theorem

$\lambda_1 \cdot \widehat{\lambda_n} \geq 1$

- Let $v \in \Lambda$ such that $\|v\| = \lambda_1$
- Let $x_1, x_2, \ldots, x_n \in \widehat{\Lambda}$ such that $\|x_n\| = \widehat{\lambda_n}$ and $\|x_i\| \leq \|x_n\|$
- **Observation:** $\exists j$ such that $\langle v, x_j \rangle \in \mathbb{Z} \setminus 0$. (**Why ?**)

$$1 \leq |\langle v, x_j \rangle| \leq \|v\| \|x_j\| \leq \lambda_1 \cdot \widehat{\lambda_n}$$

More generally, $\forall 1 \leq k \leq n$

$$1 \leq \lambda_k \cdot \widehat{\lambda_{n-k+1}} \leq n.$$

Banaszczyk Transference Theorem.

SVP in Lattice

- **(Search version):** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| = \lambda_1$.

SVP in Lattice

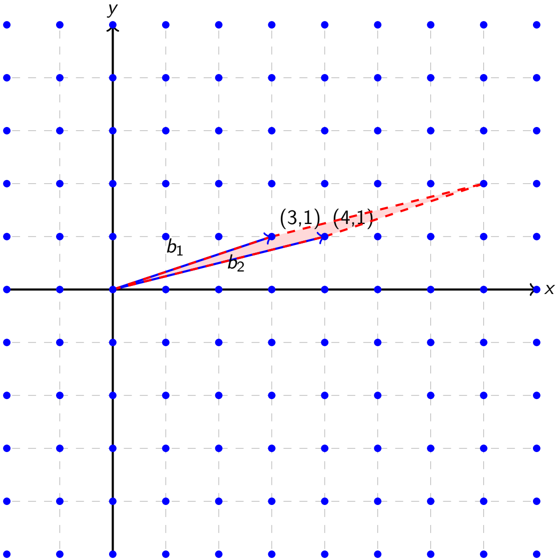
- **(Search version):** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| = \lambda_1$.
- **(Optimized version):** Given a lattice basis B, find $\lambda_1(\mathcal{L}(B))$.

SVP in Lattice

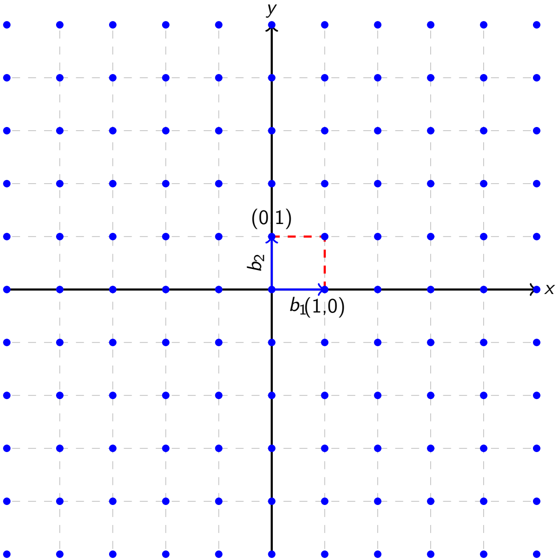
- **(Search version):** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| = \lambda_1$.
- **(Optimized version):** Given a lattice basis B, find $\lambda_1(\mathcal{L}(B))$.
- **(Decision version):** Given a lattice basis B and a real number $d > 0$, output

$$\begin{cases} \text{yes}, & \text{if } \lambda_1(\mathcal{L}(B)) \leq d \\ \text{no}, & \text{if } \lambda_1(\mathcal{L}(B)) > d \end{cases}$$

What Makes SVP Hard



What Makes SVP Hard



What Makes SVP Hard

Can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

What Makes SVP Hard

Can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

- Seems to be easy in lower dimension
- Its fairly difficult in higher dimension

What Makes SVP Hard

Can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

- Seems to be easy in lower dimension
- Its fairly difficult in higher dimension

Seeks for Lattice Basis Reduction (LLL, BKZ)

What Makes SVP Hard

Can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

- Seems to be easy in lower dimension
- Its fairly difficult in higher dimension

Seeks for Lattice Basis Reduction (LLL, BKZ)

Search-SVP $\Leftrightarrow$ Optimized-SVP $\Leftrightarrow$ Decisional-SVP

CVP in Lattice

- **(Search version):** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that v is the closest vector to t. That is,

$$\|v - t\| \leq \|v' - t\|, \quad \forall v' \in \mathcal{L}(B).$$

CVP in Lattice

- **(Search version):** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that v is the closest vector to t. That is,

$$\|v - t\| \leq \|v' - t\|, \quad \forall v' \in \mathcal{L}(B).$$

- **(Optimized version):** Given a lattice basis B and a point t, find distance(t,$\mathcal{L}(B)$).

CVP in Lattice

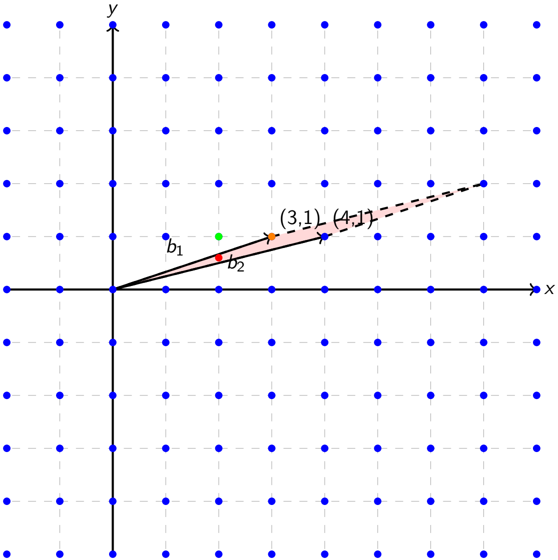
- **(Search version):** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that v is the closest vector to t. That is,

$$\|v - t\| \leq \|v' - t\|, \quad \forall v' \in \mathcal{L}(B).$$

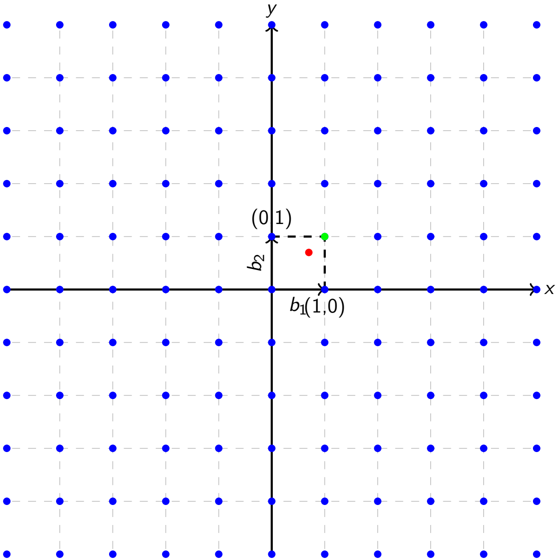
- **(Optimized version):** Given a lattice basis B and a point t, find distance(t,$\mathcal{L}(B)$).
- **(Decision version):** Given a lattice basis B ,a point t and a real number $d > 0$, then output

$$\begin{cases} \text{yes}, & \text{if } \operatorname{dist}(t, L(B)) \leq d \\ \text{no}, & \text{if } \operatorname{dist}(t, L(B)) > d \end{cases}$$

What Makes CVP Hard



What Makes CVP Hard



What Makes CVP Hard

Similar to SVP, can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

What Makes CVP Hard

Similar to SVP, can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

- Seems to be easy in lower dimension
- Its fairly difficult in higher dimension

What Makes CVP Hard

Similar to SVP, can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

- Seems to be easy in lower dimension
- Its fairly difficult in higher dimension

Seeks for Lattice Basis Reduction (LLL, BKZ) followed by Babai Nearest Plane Algorithm.

What Makes CVP Hard

Similar to SVP, can we find an unimodular transformation that transforms a given skewed basis to a orthogonal basis of the lattice ?

- Seems to be easy in lower dimension
- Its fairly difficult in higher dimension

Seeks for Lattice Basis Reduction (LLL, BKZ) followed by Babai Nearest Plane Algorithm.

Search-CVP $\Leftrightarrow$ Optimized-CVP $\Leftrightarrow$ Decisional-CVP

Approximate Variants of SVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1$.
- **(Optimized version:)** Given a lattice basis B, find a real number d such that $\lambda_1(\mathcal{L}(B)) \leq d \leq \gamma\lambda_1(\mathcal{L}(B))$.
- **(Decision version:)** Given a lattice basis B and a real number $d > 0$, then output yes if $\lambda_1(\mathcal{L}(B)) \leq d$ and no if $\lambda_1(\mathcal{L}(B)) > \gamma d$.

Approximate Variants of SVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1$.
- **(Optimized version:)** Given a lattice basis B, find a real number d such that $\lambda_1(\mathcal{L}(B)) \leq d \leq \gamma\lambda_1(\mathcal{L}(B))$.
- **(Decision version:)** Given a lattice basis B and a real number $d > 0$, then output yes if $\lambda_1(\mathcal{L}(B)) \leq d$ and no if $\lambda_1(\mathcal{L}(B)) > \gamma d$.

Approximate variant of Decisional version of SVP is also known as GapSVP$_\gamma$ problem.

Approximate Variants of SVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1$.
- **(Optimized version:)** Given a lattice basis B, find a real number d such that $\lambda_1(\mathcal{L}(B)) \leq d \leq \gamma\lambda_1(\mathcal{L}(B))$.
- **(Decision version:)** Given a lattice basis B and a real number $d > 0$, then output yes if $\lambda_1(\mathcal{L}(B)) \leq d$ and no if $\lambda_1(\mathcal{L}(B)) > \gamma d$.

Decisional-SVP$_\gamma$ $\Rightarrow$ **Optimized-SVP$_\gamma$** $\Rightarrow$ **Search-SVP$_\gamma$**

Optimized-SVP$_\gamma$ $\Rightarrow$ **Decisional-SVP$_\gamma$** (apply binary search)

Approximate Variants of SVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B, find a non-zero vector $v \in \mathcal{L}$ such that $\|v\| \leq \gamma\lambda_1$.
- **(Optimized version:)** Given a lattice basis B, find a real number d such that $\lambda_1(\mathcal{L}(B)) \leq d \leq \gamma\lambda_1(\mathcal{L}(B))$.
- **(Decision version:)** Given a lattice basis B and a real number $d > 0$, then output yes if $\lambda_1(\mathcal{L}(B)) \leq d$ and no if $\lambda_1(\mathcal{L}(B)) > \gamma d$.

Decisional-SVP$_\gamma$ $\Rightarrow$ **Optimized-SVP$_\gamma$** $\Rightarrow$ **Search-SVP$_\gamma$**

Optimized-SVP$_\gamma$ $\Rightarrow$ **Decisional-SVP$_\gamma$** (apply binary search)

Search-SVP$_\gamma$ $\Rightarrow$ **Optimized-SVP$_\gamma$** (still open)

Approximate Variants of CVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that $\|v - t\| \leq \gamma||v' - t||, \forall v' \in \mathcal{L}$.
- **(Optimized version:)** Given a lattice basis B and a point t, find a real number d such that distance(t,$\mathcal{L}(B)$)$\leq d \leq \gamma$ distance(t,$\mathcal{L}(B)$).
- **(Decision version:)** Given a lattice basis B ,a point t and a real number $d > 0$, then output yes, if distance(t,$\mathcal{L}(B)$) $\leq$ d and no, if distance(t,$\mathcal{L}(B)$)$> \gamma d$.

Approximate Variants of CVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that $\|v - t\| \leq \gamma||v' - t||, \forall v' \in \mathcal{L}$.
- **(Optimized version:)** Given a lattice basis B and a point t, find a real number d such that distance(t,$\mathcal{L}(B)$)$\leq d \leq \gamma$ distance(t,$\mathcal{L}(B)$).
- **(Decision version:)** Given a lattice basis B ,a point t and a real number $d > 0$, then output yes, if distance(t,$\mathcal{L}(B)$) $\leq$ d and no, if distance(t,$\mathcal{L}(B)$)$> \gamma d$.

Approximate variant of Decisional version of CVP is also known as GapCVP$_\gamma$ problem.

Approximate Variants of CVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that $\|v - t\| \leq \gamma ||v' - t||, \forall v' \in \mathcal{L}$.
- **(Optimized version:)** Given a lattice basis B and a point t, find a real number d such that distance(t,$\mathcal{L}(B)$)$\leq d \leq \gamma$ distance(t,$\mathcal{L}(B)$).
- **(Decision version:)** Given a lattice basis B ,a point t and a real number $d > 0$, then output yes, if distance(t,$\mathcal{L}(B)$) $\leq$ d and no, if distance(t,$\mathcal{L}(B)$)$> \gamma d$.

Decisional-CVP$_\gamma$ $\Rightarrow$ Optimized-CVP$_\gamma$ $\Rightarrow$ Search-CVP$_\gamma$

Approximate Variants of CVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that $\|v - t\| \leq \gamma||v' - t||, \forall v' \in \mathcal{L}$.
- **(Optimized version:)** Given a lattice basis B and a point t, find a real number d such that distance(t,$\mathcal{L}(B)$)$\leq d \leq \gamma$ distance(t,$\mathcal{L}(B)$).
- **(Decision version:)** Given a lattice basis B ,a point t and a real number $d > 0$, then output yes, if distance(t,$\mathcal{L}(B)$) $\leq$ d and no, if distance(t,$\mathcal{L}(B)$)$> \gamma d$.

Decisional-CVP$_\gamma$ $\Rightarrow$ **Optimized-CVP$_\gamma$** $\Rightarrow$ **Search-CVP$_\gamma$**

Optimized-CVP$_\gamma$ $\Rightarrow$ **Decisional-CVP$_\gamma$** (apply binary search)

Approximate Variants of CVP

Let γ be the approximation factor

- **(Search version:)** Given a lattice basis B and a point t (not in the lattice), find a vector v in the lattice such that $\|v - t\| \leq \gamma ||v' - t||, \forall v' \in \mathcal{L}$.
- **(Optimized version:)** Given a lattice basis B and a point t, find a real number d such that distance(t,$\mathcal{L}(B)$)$\leq d \leq \gamma$ distance(t,$\mathcal{L}(B)$).
- **(Decision version:)** Given a lattice basis B ,a point t and a real number $d > 0$, then output yes, if distance(t,$\mathcal{L}(B)$) $\leq$ d and no, if distance(t,$\mathcal{L}(B)$)$> \gamma d$.

Decisional-CVP$_\gamma$ $\Rightarrow$ **Optimized-CVP$_\gamma$** $\Rightarrow$ **Search-CVP$_\gamma$**

Optimized-CVP$_\gamma$ $\Rightarrow$ **Decisional-CVP$_\gamma$** (apply binary search)

Search-CVP$_\gamma$ $\Rightarrow$ **Optimized-CVP$_\gamma$** (still open)

Thank You!