

CSE206A: Lattice Algorithms and Applications

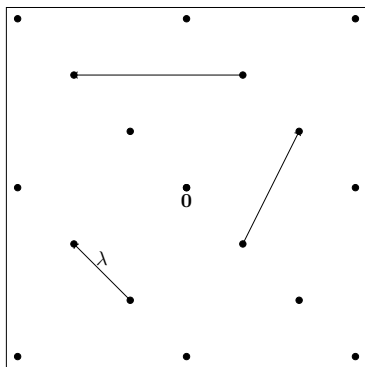
Lecture 2

Shortest Vector Problem

UCSD – Fall 2025

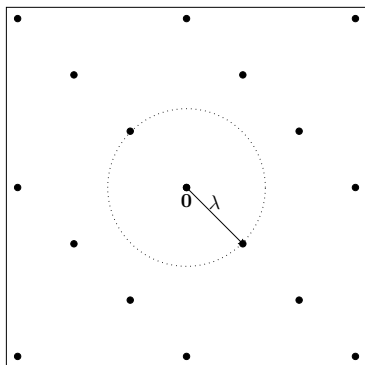
Daniele Micciancio





- Lattice $\mathcal{L}$, usually represented by a basis
- Minimum distance: $\lambda(\mathcal{L}) = \min \{\|x - y\| : x, y \in \mathcal{L}, x \neq y\}$
- Assume WLOG that $x = 0$:

$$\lambda(\mathcal{L}) = \min \{\|x\| : x \in \mathcal{L} \setminus \{0\}\}$$



- SVP (Shortest vector Problem): Find the (length of the) shortest nonzero vector in a given lattice $\mathcal{L}$
 - Search: Find $x \in \mathcal{L}$
 - Optimization: Find $\lambda(\mathcal{L})$
 - Decision: Given $(\mathcal{L}, t)$, decide if $\lambda(\mathcal{L}) \leq t$

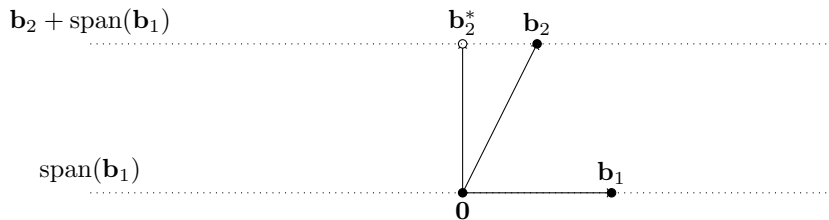
- Any (finite dimensional) vector space has an orthogonal basis

- Given an arbitrary basis $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^n$

- For any $i = 1, \dots, n$, let $\mathbf{b}_i^*$ be the component of $\mathbf{b}_i$ orthogonal to $\mathbf{b}_1, \dots, \mathbf{b}_{i-1}$

- $\mathbf{b}_2^* = \mathbf{b}_2 - \mu \mathbf{b}_1$

- $\mu = \frac{\langle \mathbf{b}_2, \mathbf{b}_1 \rangle}{\langle \mathbf{b}_1, \mathbf{b}_1 \rangle}$



- More generally $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j < i} \mu_{i,j} \mathbf{b}_j^*$ where $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$
- $B = B^* M$ where M is a “unitriangular” matrix with coefficients $\mu_{i,j}$

- $\mathbf{b}_1^*, \dots, \mathbf{b}_n^*$ gives an orthogonal basis for the same vector space as $\mathbf{b}_1, \dots, \mathbf{b}_n$
 - $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_i) = \text{span}(\mathbf{b}_1^*, \dots, \mathbf{b}_i^*)$ for all $i = 1, \dots, n$
 - $\langle \mathbf{b}_i, \mathbf{b}_j \rangle = 0$ for all $i \neq j$
- However, $\Lambda = \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n) \neq \mathcal{L}(\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ are usually different lattices
 - $\mathbf{b}_1^* = \mathbf{b}_1 \in \Lambda$ by definition
 - but $\mathbf{b}_2^*$ may not belong to Λ

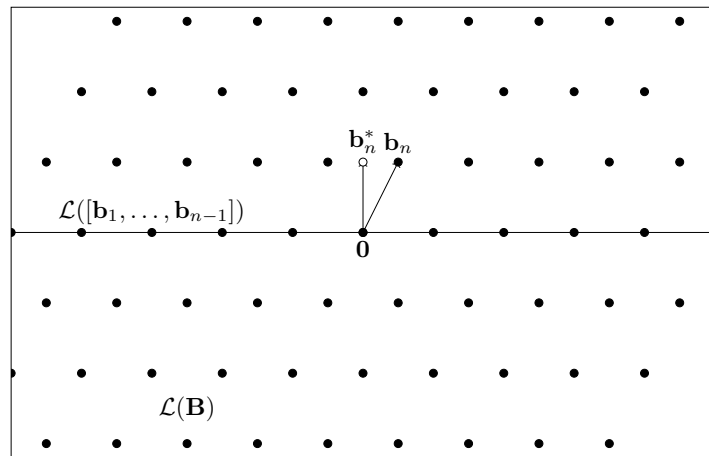
Exercise 1. Give a basis $[\mathbf{b}_1, \mathbf{b}_2]$ such that $\mathcal{L}(\mathbf{b}_1, \mathbf{b}_2) \neq \mathcal{L}(\mathbf{b}_1^*, \mathbf{b}_2^*)$

Exercise 2. Give a basis $[\mathbf{b}_1, \mathbf{b}_2]$ such that $[\mathbf{b}_1, \mathbf{b}_2] \neq [\mathbf{b}_1^*, \mathbf{b}_2^*]$ and still $\mathcal{L}(\mathbf{b}_1, \mathbf{b}_2) = \mathcal{L}(\mathbf{b}_1^*, \mathbf{b}_2^*)$

Question 1. Is there an “integer” variant of GSO for “approximate” orthogonalization?

Theorem 1. For any lattice basis B , the minimum distance is $\lambda(B) \geq \min \|b_i^*\|$

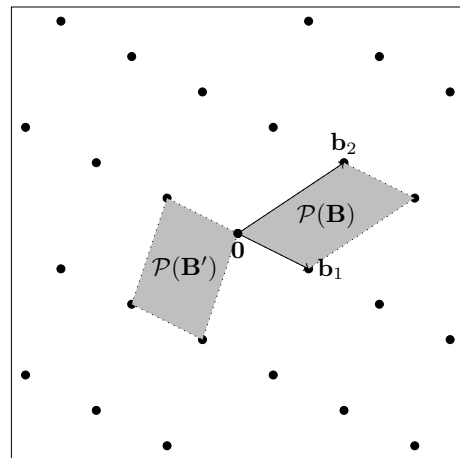
- Fix a basis $B = [B', b_n]$
- Partition $\mathcal{L}(B) = \mathcal{L}(B') + \mathbb{Z} b_n$ into layers
- If the shortest vector in $\mathcal{L}(B')$ then $\lambda \geq \min \|b_i^*\|$ by induction
- If the shortest vector is in $\mathcal{L}(B') + c b_n$ with $c \neq 0$, then $\lambda \geq \|b_n^*\|$



- Fundamental region/parallelepiped of basis $\mathbf{B}$

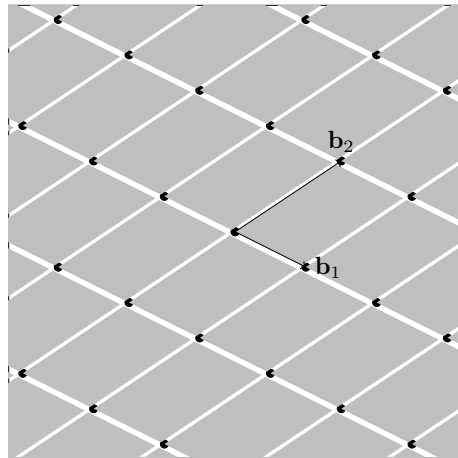
$$\mathcal{P}(\mathbf{B}) = \{\sum_{i=1}^n x_i \mathbf{b}_i : \forall i. 0 \leq x_i < 1\}$$

- Different bases give different regions
- All fundamental regions have the same volume
- The lattice determinant $\det(\mathcal{L}(\mathbf{B}))$
 - volume of $\mathcal{P}(\mathbf{B})$, does not depend on choice of basis $\mathbf{B}$
 - For $\mathbf{B} \in \mathbb{R}^{n \times n}$, same as matrix determinant $|\det(\mathbf{B})|$
 - $\det(\mathbf{B}\mathbf{U}) = \det(\mathbf{B}) \det(\mathbf{U}) = \pm \det(\mathbf{B})$



- Every point in space is the sum $\mathbf{v} + \mathbf{x}$ of
 1. a lattice point $\mathbf{v} \in \mathcal{L}(\mathbf{B})$, and
 2. an offset $\mathbf{x} \in \mathcal{P}(\mathbf{B})$
- $\{\mathbf{v} + \mathcal{P}(\mathbf{B})\}_{\mathbf{v} \in \mathcal{L}(\mathbf{B})}$ is a partition of $\text{span}(\mathbf{B})$
- One lattice point for every region of volume $\det(\mathcal{P}(\mathbf{B}))$
- Center density of lattice Λ :

$$\lim_{r \rightarrow \infty} \frac{\#\{\mathbf{v} \in \Lambda: \|\mathbf{v}\| \leq r\}}{\text{vol}(\{\mathbf{x}: \|\mathbf{x}\| \leq r\})} = \frac{1}{\det(\Lambda)}$$

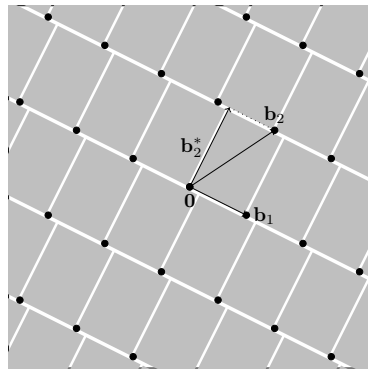
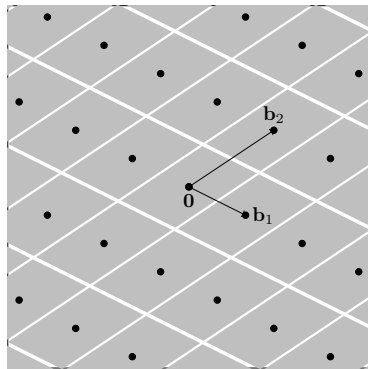


- Centered parallelepiped

$$\mathcal{C}(\mathbf{B}) = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i : \forall i. x_i \in \left[-\frac{1}{2}, \frac{1}{2}\right) \right\}$$

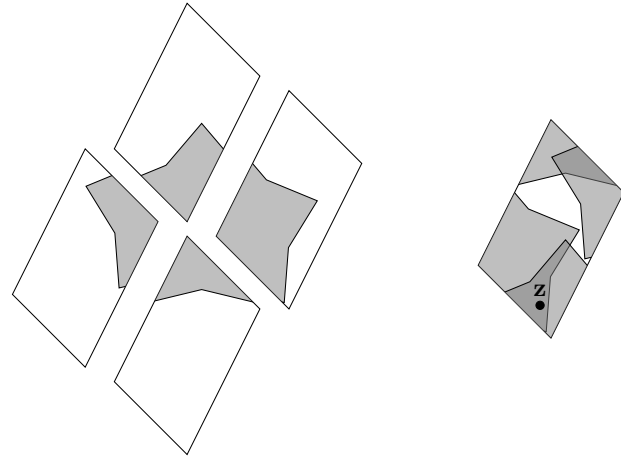
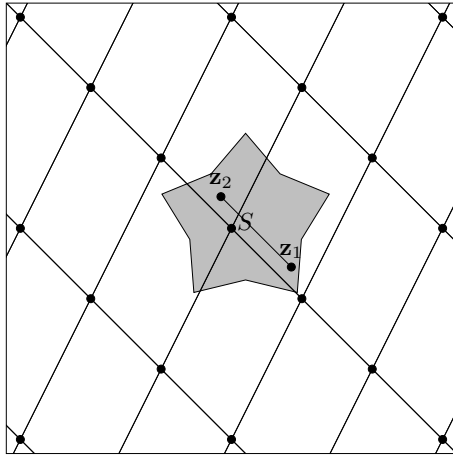
- Orthogonalized parallelepiped

$$\mathcal{P}(\mathbf{B}^*) = \left\{ \sum_{i=1}^n x_i \mathbf{b}_i^* : \forall i. x_i \in [0, 1) \right\}$$



- $\det(\mathbf{B})$ is easily computed from GSO: $\det(\mathbf{B}) = \det(\mathbf{B}^* \mathbf{M}) = \det(\mathbf{B}^*) = \prod_i \|\mathbf{b}_i^*\|$
- Hadamard inequality: $\det(\mathbf{B}) = \prod_i \|\mathbf{b}_i^*\| \leq \prod_i \|\mathbf{b}_i\|$
- If $\mathbf{B} \in \mathbb{Z}^{n \times n}$ and $\mathbf{H} = \text{HNF}(\mathbf{B})$, then $\det(\mathbf{B}) = \det(\mathbf{H}) = \prod_i h_{i,i}$

Theorem 2. (Blichfeldt) For any lattice Λ and (measurable) set S , if $\text{vol}(S) > \det(\Lambda)$ then S contains two points $z_1, z_2 \in S$ such that $z_1 - z_2 \in L$



Theorem 3. *If S is a symmetric convex body of volume $\text{vol}(S) \geq 2^n \det(\Lambda)$, then S contains a nonzero lattice point*

Proof. Apply Blichfeldt Theorem to $\frac{1}{2}S$:

1. Since $\text{vol}\left(\frac{1}{2}S\right) \geq \det(\Lambda)$, $\exists z_1, z_2 \in S/2, z_1 - z_2 \in \Lambda$
2. $2z_1, 2z_2 \in S$, also $-2z_2 \in \Lambda$ (by symmetry)
3. $z_1 - z_2 = \frac{1}{2}(2z_1 + (-2z_2)) \in S$ (by convexity)

□

Using $S = \{x: \|x\|_\infty \leq \det(\Lambda)^{1/n}\}$, $\text{vol}(S) = 2^n \det(\Lambda)$

we get $\lambda(\Lambda) \leq \sqrt{n} \det(\Lambda)^{1/n}$

