Introduction to lattices

Damien Stehlé

ÉNS de Lyon

EPIT, Autrans, March 2013

Lattices in computer science

- Lattices are a fairly old mathematical object.
- But still quite poorly understood.

- Their computational aspects have been studied for $>$30 years.
- But many important computational questions remain open.
  $\Rightarrow$ Not so many algorithms **[Guillaume]**
  $\Rightarrow$ Even the simplest algorithms are hard to analyze **[Brigitte]**

- Used in many areas, including:
  - Communications theory **[Jean-Claude]**
  - Cryptography **[Mehdi & Vadim]**
  - Computer arithmetic **[Nicolas]**
  - Convex geometry **[Daniel]**

Lattices in computer science

- Lattices are a fairly old mathematical object.
- But still quite poorly understood.

- Their computational aspects have been studied for >30 years.
- But many important computational questions remain open.
  $\Rightarrow$ Not so many algorithms **[Guillaume]**
  $\Rightarrow$ Even the simplest algorithms are hard to analyze **[Brigitte]**

- Used in many areas, including:
  - Communications theory **[Jean-Claude]**
  - Cryptography **[Mehdi & Vadim]**
  - Computer arithmetic **[Nicolas]**
  - Convex geometry **[Daniel]**

Lattices in computer science

- Lattices are a fairly old mathematical object.
- But still quite poorly understood.

- Their computational aspects have been studied for >30 years.
- But many important computational questions remain open.
  $\Rightarrow$ Not so many algorithms **[Guillaume]**
  $\Rightarrow$ Even the simplest algorithms are hard to analyze **[Brigitte]**

- Used in many areas, including:
  - Communications theory **[Jean-Claude]**
  - Cryptography **[Mehdi & Vadim]**
  - Computer arithmetic **[Nicolas]**
  - Convex geometry **[Daniel]**

Objectives

Goals of the week:

- An introduction to the computational aspects of lattices.
- An overview of active research fields involving lattices.

Goals of this first lecture:

- Give the mathematical background.
- Describe how to handle the basic computational tasks.

Objectives

Goals of the week:

- An introduction to the computational aspects of lattices.
- An overview of active research fields involving lattices.

Goals of this first lecture:

- Give the mathematical background.
- Describe how to handle the basic computational tasks.

My favorite sources for the material of this lecture

- Oded Regev's lecture notes:
  `http://www.cims.nyu.edu/~regev/teaching/`
- Daniele Micciancio's lecture notes:
  `http://cseweb.ucsd.edu/~daniele/classes.html/`

Outline

1. Lattices and lattice bases.
2. Lattice invariants.
3. Examples of lattices.
4. Gram-Schmidt orthogonalisation.
5. Lattice Gaussians.
6. Computational problems on lattices.

Outline

1. **Lattices and lattice bases.**
2. Lattice invariants.
3. Examples of lattices.
4. Gram-Schmidt orthogonalisation.
5. Lattice Gaussians.
6. Computational problems on lattices.

A first definition

Algebraic definition of a lattice

A lattice L is a discrete additive subgroup of an $\mathbb{R}^n$.

- Additive subgroup:
  L is stable under integral linear combinations.
- Discrete: no accumulation point.
  For any $\mathbf{b} \in L$, there is a ball around $\mathbf{b}$ containing only $\mathbf{b}$.

A first definition

Algebraic definition of a lattice

A lattice L is a discrete additive subgroup of an $\mathbb{R}^n$.

- Additive subgroup:
  L is stable under integral linear combinations.
- Discrete: no accumulation point.
  For any $\mathbf{b} \in L$, there is a ball around $\mathbf{b}$ containing only $\mathbf{b}$.

A first definition

Algebraic definition of a lattice

A lattice L is a discrete additive subgroup of an $\mathbb{R}^n$.

- Additive subgroup:
  L is stable under integral linear combinations.
- Discrete: no accumulation point.
  For any $\mathbf{b} \in L$, there is a ball around $\mathbf{b}$ containing only $\mathbf{b}$.

First examples

Examples of lattices

- $\mathbb{Z} \subseteq \mathbb{R}$.
- $\mathbb{Z}^d \subseteq \mathbb{R}^n$ with $d \leq n$.
- Any subgroup of $\mathbb{Z}^d$.

Counter-example

- $S = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ is not a lattice:
  if $(p_k/q_k)_k$ are the continued fraction convergents of $\sqrt{2}$, then

$$\begin{aligned} p_k - q_k\sqrt{2} &\rightarrow_k 0, \\ p_k - q_k\sqrt{2} &\in S \setminus 0. \end{aligned}$$

First examples

Examples of lattices

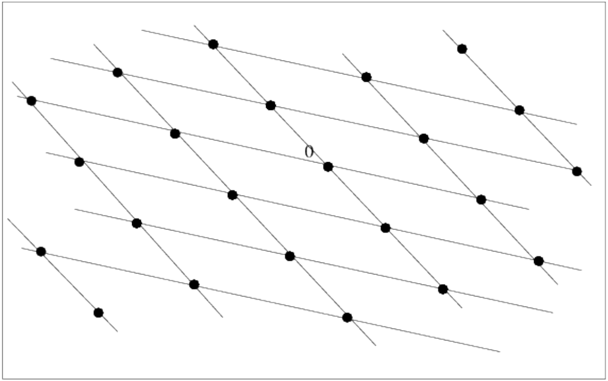
- $\mathbb{Z} \subseteq \mathbb{R}$.
- $\mathbb{Z}^d \subseteq \mathbb{R}^n$ with $d \leq n$.
- Any subgroup of $\mathbb{Z}^d$.

Counter-example

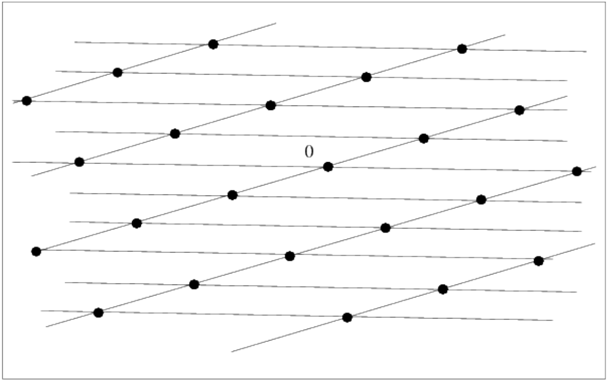
- $S = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ is not a lattice:
  if $(p_k/q_k)_k$ are the continued fraction convergents of $\sqrt{2}$, then

$$\begin{array}{rcl} p_k - q_k\sqrt{2} & \to_k & 0, \\ p_k - q_k\sqrt{2} & \in & S \setminus 0. \end{array}$$

A 2-dimensional lattice



The same lattice



An equivalent definition

Constructive definition of a lattice

A lattice L is the set of all integer linear combinations of some linearly independent vectors in an $\mathbb{R}^n$.

$$L = \sum_{1 \le i \le d} \mathbb{Z}\mathbf{b}_i = \{ \sum_{1 \le i \le d} x_i \mathbf{b}_i, x_i \in \mathbb{Z} \} = B \cdot \mathbb{Z}^d,$$

where the $\mathbf{b}_i$'s are linearly independent vectors of $\mathbb{R}^n$,
and $B \in \mathbb{R}^{n \times d}$ is the matrix whose columns are the $\mathbf{b}_i$'s.

- $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is a basis of L. It is not unique.
- Embedding dimension: n (a trivial invariant of L).
- Lattice dimension: d (also an invariant of L).

If $d = n$, we say that the lattice is full-rank.

An equivalent definition

Constructive definition of a lattice

A lattice L is the set of all integer linear combinations of some linearly independent vectors in an $\mathbb{R}^n$.

$$L = \sum_{1 \leq i \leq d} \mathbb{Z}\mathbf{b}_i = \{ \sum_{1 \leq i \leq d} x_i \mathbf{b}_i, x_i \in \mathbb{Z}\} = B \cdot \mathbb{Z}^d,$$

where the $\mathbf{b}_i$'s are linearly independent vectors of $\mathbb{R}^n$,
and $B \in \mathbb{R}^{n \times d}$ is the matrix whose columns are the $\mathbf{b}_i$'s.

- $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is a basis of L. It is not unique.
- Embedding dimension: n (a trivial invariant of L).
- Lattice dimension: d (also an invariant of L).

If $d = n$, we say that the lattice is full-rank.

An equivalent definition

Constructive definition of a lattice

A lattice L is the set of all integer linear combinations of some linearly independent vectors in an $\mathbb{R}^n$.

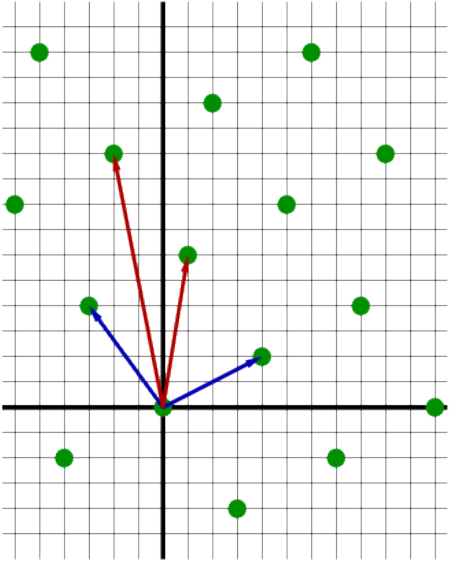
$$L = \sum_{1\leq i\leq d} \mathbb{Z}\mathbf{b}_i = \{ \sum_{1\leq i\leq d} x_i\mathbf{b}_i, x_i \in \mathbb{Z}\} = B \cdot \mathbb{Z}^d,$$

where the $\mathbf{b}_i$'s are linearly independent vectors of $\mathbb{R}^n$,
and $B \in \mathbb{R}^{n\times d}$ is the matrix whose columns are the $\mathbf{b}_i$'s.

- $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is a basis of L. It is not unique.
- Embedding dimension: n (a trivial invariant of L).
- Lattice dimension: d (also an invariant of L).

If $d = n$, we say that the lattice is full-rank.

Two bases of a 2-dimensional lattice



Relationships between bases of a given lattice

Unimodular matrices

A matrix $U \in \mathbb{Z}^{d \times d}$ is said unimodular if it is invertible over $\mathbb{Z}^{d \times d}$.
Equivalently: its determinant is $\det U = \pm 1$.
Equivalently: it belongs to $\mathrm{GL}_d(\mathbb{Z})$.

Unimodularity and lattice bases

Two bases $(\mathbf{b}_i)_{i \leq d}$ and $(\mathbf{c}_i)_{i \leq d}$ span the same lattice iff there exists $U \in \mathrm{GL}_d(\mathbb{Z})$ such that $(\mathbf{b}_i)_{i \leq d} \cdot U = (\mathbf{c}_i)_{i \leq d}$.

Direct consequences:

- Any lattice of dimension ≥ 2 has infinitely many bases.
- The set lattices of dim d is isomorphic to $GL_d(\mathbb{R})/GL_d(\mathbb{Z})$.

Relationships between bases of a given lattice

Unimodular matrices

A matrix $U \in \mathbb{Z}^{d \times d}$ is said unimodular if it is invertible over $\mathbb{Z}^{d \times d}$.
Equivalently: its determinant is $\det U = \pm 1$.
Equivalently: it belongs to $\mathrm{GL}_d(\mathbb{Z})$.

Unimodularity and lattice bases

Two bases $(\mathbf{b}_i)_{i \leq d}$ and $(\mathbf{c}_i)_{i \leq d}$ span the same lattice iff there exists $U \in \mathrm{GL}_d(\mathbb{Z})$ such that $(\mathbf{b}_i)_{i \leq d} \cdot U = (\mathbf{c}_i)_{i \leq d}$.

Direct consequences:

- Any lattice of dimension ≥ 2 has infinitely many bases.
- The set lattices of dim d is isomorphic to $GL_d(\mathbb{R})/GL_d(\mathbb{Z})$.

Relationships between bases of a given lattice

Unimodular matrices

A matrix $U \in \mathbb{Z}^{d \times d}$ is said unimodular if it is invertible over $\mathbb{Z}^{d \times d}$.
Equivalently: its determinant is $\det U = \pm 1$.
Equivalently: it belongs to $\mathrm{GL}_d(\mathbb{Z})$.

Unimodularity and lattice bases

Two bases $(\mathbf{b}_i)_{i \leq d}$ and $(\mathbf{c}_i)_{i \leq d}$ span the same lattice iff there exists $U \in \mathrm{GL}_d(\mathbb{Z})$ such that $(\mathbf{b}_i)_{i \leq d} \cdot U = (\mathbf{c}_i)_{i \leq d}$.

Direct consequences:

- Any lattice of dimension ≥ 2 has infinitely many bases.
- The set lattices of dim d is isomorphic to $GL_d(\mathbb{R})/GL_d(\mathbb{Z})$.

Duality

The dual of the d-dimensional lattice L is:

$$\begin{aligned} \widehat{L} &= \{\mathbf{c} \in \mathrm{Span}(L) : \forall \mathbf{b} \in L, \langle \mathbf{c}, \mathbf{b} \rangle \in \mathbb{Z}\} \\ &= \{\mathbf{c} \in \mathrm{Span}(L) : \mathbf{c}^T \cdot L \subseteq \mathbb{Z}^d\}. \end{aligned}$$

Dual basis

B basis matrix of L $\Rightarrow$ $\widehat{B} = B(B^T B)^{-1}$ basis matrix of $\widehat{L}$.
If L is full-rank, then $\widehat{B} = B^{-T}$.

Consequences:

- $\dim(\widehat{L}) = \dim(L)$.
- $\widehat{\widehat{L}} = L$.

Duality

The dual of the d-dimensional lattice L is:

$$\begin{aligned}\widehat{L} &= \{\mathbf{c} \in \mathrm{Span}(L) : \forall \mathbf{b} \in L, \langle \mathbf{c}, \mathbf{b} \rangle \in \mathbb{Z}\} \\ &= \{\mathbf{c} \in \mathrm{Span}(L) : \mathbf{c}^T \cdot L \subseteq \mathbb{Z}^d\}.\end{aligned}$$

Dual basis

B basis matrix of L $\Rightarrow$ $\widehat{B} = B(B^T B)^{-1}$ basis matrix of $\widehat{L}$.
If L is full-rank, then $\widehat{B} = B^{-T}$.

Consequences:

- $\dim(\widehat{L}) = \dim(L)$.
- $\widehat{\widehat{L}} = L$.

Duality

The dual of the d-dimensional lattice L is:

$$\begin{aligned}\widehat{L} &= \{\mathbf{c} \in \mathrm{Span}(L) : \forall \mathbf{b} \in L, \langle \mathbf{c}, \mathbf{b} \rangle \in \mathbb{Z}\} \\ &= \{\mathbf{c} \in \mathrm{Span}(L) : \mathbf{c}^T \cdot L \subseteq \mathbb{Z}^d\}.\end{aligned}$$

Dual basis

B basis matrix of L $\Rightarrow$ $\widehat{B} = B(B^T B)^{-1}$ basis matrix of $\widehat{L}$.
If L is full-rank, then $\widehat{B} = B^{-T}$.

Consequences:

- $\dim(\widehat{L}) = \dim(L)$.
- $\widehat{\widehat{L}} = L$.

Set operations on lattices

Let $L_1, L_2 \subseteq \mathbb{R}^n$ be two lattices.

- The union $L_1 \cup L_2$ may not be a lattice: $2\mathbb{Z} \cup 3\mathbb{Z}$.
- The $\mathbb{Z}$-span of $L_1 \cup L_2$, i.e., the sum $L_1 + L_2 = \{\mathbf{b}_1 + \mathbf{b}_2 : \mathbf{b}_1 \in L_1, \mathbf{b}_2 \in L_2\}$, may not be a lattice:

$$\mathbb{Z} + \sqrt{2}\mathbb{Z}.$$

- If $L_1, L_2 \subseteq L$ for some lattice L, then $L_1 + L_2$ is a lattice.
- The intersection $L_1 \cap L_2$ is always a lattice.
- If $\dim L_1 = \dim L_2 = \dim L_1 \cap L_2$, then:

$$L_1 \cap L_2 = \widehat{\widehat{L_1} + \widehat{L_2}}.$$

Set operations on lattices

Let $L_1, L_2 \subseteq \mathbb{R}^n$ be two lattices.

- The union $L_1 \cup L_2$ may not be a lattice: $2\mathbb{Z} \cup 3\mathbb{Z}$.
- The $\mathbb{Z}$-span of $L_1 \cup L_2$, i.e., the sum $L_1 + L_2 = \{\mathbf{b}_1 + \mathbf{b}_2 : \mathbf{b}_1 \in L_1, \mathbf{b}_2 \in L_2\}$, may not be a lattice:

$$\mathbb{Z} + \sqrt{2}\mathbb{Z}.$$

- If $L_1, L_2 \subseteq L$ for some lattice L, then $L_1 + L_2$ is a lattice.
- The intersection $L_1 \cap L_2$ is always a lattice.
- If $\dim L_1 = \dim L_2 = \dim L_1 \cap L_2$, then:

$$L_1 \cap L_2 = \widehat{\widehat{L_1} + \widehat{L_2}}.$$

Set operations on lattices

Let $L_1, L_2 \subseteq \mathbb{R}^n$ be two lattices.

- The union $L_1 \cup L_2$ may not be a lattice: $2\mathbb{Z} \cup 3\mathbb{Z}$.
- The $\mathbb{Z}$-span of $L_1 \cup L_2$, i.e., the sum $L_1 + L_2 = \{\mathbf{b}_1 + \mathbf{b}_2 : \mathbf{b}_1 \in L_1, \mathbf{b}_2 \in L_2\}$, may not be a lattice:

$$\mathbb{Z} + \sqrt{2}\mathbb{Z}.$$

- If $L_1, L_2 \subseteq L$ for some lattice L, then $L_1 + L_2$ is a lattice.
- The intersection $L_1 \cap L_2$ is always a lattice.
- If $\dim L_1 = \dim L_2 = \dim L_1 \cap L_2$, then:

$$L_1 \cap L_2 = \widehat{\widehat{L_1} + \widehat{L_2}}.$$

Computing a basis of the sum of lattices

Let B_1, B_2 be bases of lattices $L_1, L_2 \subseteq \mathbb{Z}^n$.
How can we compute a basis of $L_1 + L_2$?

Hermite Normal Form (HNF)

For any $X \in \mathbb{Z}^{m \times n}$, there exists $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $X \cdot U = (L|0)$ with L lower trapezoidal.

- That's akin to Gauss' pivoting for linear systems.
- Can be performed efficiently (see, e.g., [Micciancio-Warinschi'01])
- In our case, use $X = (B_1|B_2)$, and L is a basis matrix for $L_1 + L_2$.

Computing a basis of the sum of lattices

Let B_1, B_2 be bases of lattices $L_1, L_2 \subseteq \mathbb{Z}^n$.
How can we compute a basis of $L_1 + L_2$?

Hermite Normal Form (HNF)

For any $X \in \mathbb{Z}^{m \times n}$, there exists $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $X \cdot U = (L|0)$ with L lower trapezoidal.

- That's akin to Gauss' pivoting for linear systems.
- Can be performed efficiently (see, e.g., [Micciancio-Warinschi'01])
- In our case, use $X = (B_1|B_2)$, and L is a basis matrix for $L_1 + L_2$.

Computing a basis of the sum of lattices

Let B_1, B_2 be bases of lattices $L_1, L_2 \subseteq \mathbb{Z}^n$.
How can we compute a basis of $L_1 + L_2$?

Hermite Normal Form (HNF)

For any $X \in \mathbb{Z}^{m \times n}$, there exists $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $X \cdot U = (L|0)$ with L lower trapezoidal.

- That's akin to Gauss' pivoting for linear systems.
- Can be performed efficiently (see, e.g., [Micciancio-Warinschi'01])
- In our case, use $X = (B_1|B_2)$, and L is a basis matrix for $L_1 + L_2$.

Outline

1. Lattices and lattice bases.
2. **Lattice invariants.**
3. Examples of lattices.
4. Gram-Schmidt orthogonalisation.
5. Lattice Gaussians.
6. Computational problems on lattices.

The lattice minimum

Lattice minimum

For any lattice $L \neq 0$, there exists a vector $\mathbf{b}$ in L of shortest non-zero norm. The norm of that vector is the minimum $\lambda_1(L)$:

$$\lambda_1(L) = \min\left(r : \mathcal{B}(\mathbf{0}, r) \cap L \neq \{\mathbf{0}\}\right).$$

- By default, one considers the euclidean norm.
- The minimum is always reached at least twice.
- It may be reached exponentially many times.

The lattice minimum

Lattice minimum

For any lattice $L \neq 0$, there exists a vector $\mathbf{b}$ in L of shortest non-zero norm. The norm of that vector is the minimum $\lambda_1(L)$:

$$\lambda_1(L) = \min\left(r : \mathcal{B}(\mathbf{0}, r) \cap L \neq \{\mathbf{0}\}\right).$$

- By default, one considers the euclidean norm.
- The minimum is always reached at least twice.
- It may be reached exponentially many times.

The lattice minimum

Lattice minimum

For any lattice $L \neq 0$, there exists a vector $\mathbf{b}$ in L of shortest non-zero norm. The norm of that vector is the minimum $\lambda_1(L)$:

$$\lambda_1(L) = \min\left(r : \mathcal{B}(\mathbf{0}, r) \cap L \neq \{\mathbf{0}\}\right).$$

- By default, one considers the euclidean norm.
- The minimum is always reached at least twice.
- It may be reached exponentially many times.

The lattice minimum

Lattice minimum

For any lattice $L \neq 0$, there exists a vector $\mathbf{b}$ in L of shortest non-zero norm. The norm of that vector is the minimum $\lambda_1(L)$:

$$\lambda_1(L) = \min\left(r : \mathcal{B}(\mathbf{0}, r) \cap L \neq \{\mathbf{0}\}\right).$$

- By default, one considers the euclidean norm.
- The minimum is always reached at least twice.
- It may be reached exponentially many times.

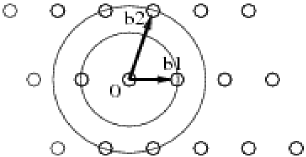
Successive minima

The first minimum measures "sparseness" only wrt one dimension.

Successive minima

For $i \leq d$, the ith minimum of a d-dimensional lattice L is:

$$\lambda_i(L) = \min\left(r : \dim \operatorname{span}(\mathcal{B}(\mathbf{0}, r) \cap L) \geq i\right).$$



Banaszczyk's transference theorem

For any d-dimensional lattice L: $\lambda_1(L) \cdot \lambda_d(\widehat{L}) \leq d$.

(obtained using Fourier analysis – see Daniel's talk)

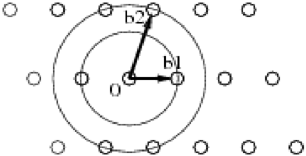
Successive minima

The first minimum measures "sparseness" only wrt one dimension.

Successive minima

For $i \leq d$, the ith minimum of a d-dimensional lattice L is:

$$\lambda_i(L) = \min\left(r : \dim \operatorname{span}(\mathcal{B}(\mathbf{0}, r) \cap L) \geq i\right).$$



Banaszczyk's transference theorem

For any d-dimensional lattice L: $\lambda_1(L) \cdot \lambda_d(\widehat{L}) \leq d$.

(obtained using Fourier analysis – see Daniel's talk)

Correct and incorrect properties on the successive minima

The minima can be reached by lin. indep. vectors

Then there exist $\mathbf{s}_1, \ldots, \mathbf{s}_d \in L$ linearly independent such that:

$$\forall i \leq d : \|\mathbf{s}_i\| = \lambda_i(L).$$

- There are lattices for which no basis reaches the minima.
- There are lattices where the shortest bases are $\Theta(\sqrt{d})$ larger than the minima:

$$\begin{bmatrix} 2 & 0 & \ldots & 0 & 1 \\ 0 & 2 & \ldots & 0 & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}$$

Correct and incorrect properties on the successive minima

The minima can be reached by lin. indep. vectors

Then there exist $\mathbf{s}_1, \ldots, \mathbf{s}_d \in L$ linearly independent such that:

$$\forall i \leq d : \|\mathbf{s}_i\| = \lambda_i(L).$$

- There are lattices for which no basis reaches the minima.
- There are lattices where the shortest bases are $\Theta(\sqrt{d})$ larger than the minima:

$$\begin{bmatrix} 2 & 0 & \ldots & 0 & 1 \\ 0 & 2 & \ldots & 0 & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}$$

Lattice determinant

The Gram matrix of a basis $(\mathbf{b}_i)_{i \leq d}$ is $G = (\langle \mathbf{b}_i, \mathbf{b}_j \rangle)_{i,j} = B^T B$.

Determinant of a lattice

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of a lattice L. We define:

$$\det(L) = \sqrt{\det(G(\mathbf{b}_1, \ldots, \mathbf{b}_d))}.$$

Simple properties:

- The determinant is a lattice invariant.
- If L is full-rank, then $\det(L) = |\det B|$.
- Hadamard: $\det(L) \leq \prod_i \|\mathbf{b}_i\|$ for any basis.
- $\det(\widehat{L}) = 1/\det(L)$.
- If $L \subseteq L'$ are full-rank, then $\det(L') | \det(L)$.
  L'/L is a finite additive group of cardinality $\det(L)/\det(L')$.

Lattice determinant

The Gram matrix of a basis $(\mathbf{b}_i)_{i\leq d}$ is $G = (\langle \mathbf{b}_i, \mathbf{b}_j\rangle)_{i,j} = B^T B$.

Determinant of a lattice

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of a lattice L. We define:

$$\det(L) = \sqrt{\det(G(\mathbf{b}_1, \ldots, \mathbf{b}_d))}.$$

Simple properties:

- The determinant is a lattice invariant.
- If L is full-rank, then $\det(L) = |\det B|$.
- Hadamard: $\det(L) \leq \prod_i \|\mathbf{b}_i\|$ for any basis.
- $\det(\widehat{L}) = 1/\det(L)$.
- If $L \subseteq L'$ are full-rank, then $\det(L') | \det(L)$.
  L'/L is a finite additive group of cardinality $\det(L)/\det(L')$.

Lattice determinant

The Gram matrix of a basis $(\mathbf{b}_i)_{i \leq d}$ is $G = (\langle \mathbf{b}_i, \mathbf{b}_j \rangle)_{i,j} = B^T B$.

Determinant of a lattice

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of a lattice L. We define:

$$\det(L) = \sqrt{\det(G(\mathbf{b}_1, \ldots, \mathbf{b}_d))}.$$

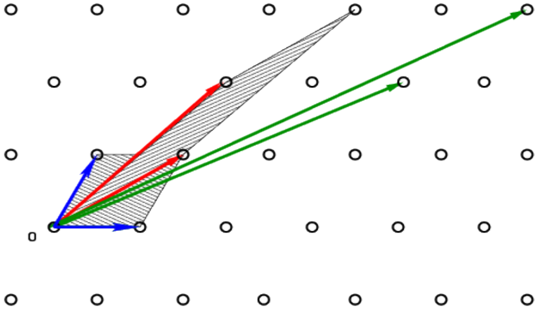
Simple properties:

- The determinant is a lattice invariant.
- If L is full-rank, then $\det(L) = |\det B|$.
- Hadamard: $\det(L) \leq \prod_i \|\mathbf{b}_i\|$ for any basis.
- $\det(\widehat{L}) = 1/\det(L)$.
- If $L \subseteq L'$ are full-rank, then $\det(L') | \det(L)$.
  L'/L is a finite additive group of cardinality $\det(L)/\det(L')$.

Geometric interpretation of the determinant

The determinant of a lattice L with basis $(\mathbf{b}_i)_{i \leq d}$ is the volume of the parallelepiped spanned by the basis vectors.

It also quantifies the d-dimensional sparseness of the lattice.



Minkowski's theorems

Provides a relationship between the invariants we have seen so far.

Minkowski's theorem

Let $L \subseteq \mathbb{R}^n$ be a full-rank lattice and $S \subseteq \mathbb{R}^n$ convex and symmetric with $\mathrm{vol}(S) > 2^n \cdot \det(L)$. Then there is $x \in (L \setminus 0) \cap S$. If S is closed, it suffices that $\mathrm{vol}(S) \geq 2^n \cdot \det(L)$.

Corollary 1

For any n-dimensional lattice L, we have: $\lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

Corollary 2

For any n-dimensional lattice L, we have:

$$\prod_{i \leq n} \lambda_i(L) \leq \sqrt{n}^n \cdot \det(L).$$

Minkowski's theorems

Provides a relationship between the invariants we have seen so far.

Minkowski's theorem

Let $L \subseteq \mathbb{R}^n$ be a full-rank lattice and $S \subseteq \mathbb{R}^n$ convex and symmetric with $\mathrm{vol}(S) > 2^n \cdot \det(L)$. Then there is $x \in (L \setminus 0) \cap S$. If S is closed, it suffices that $\mathrm{vol}(S) \geq 2^n \cdot \det(L)$.

Corollary 1

For any n-dimensional lattice L, we have: $\lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

Corollary 2

For any n-dimensional lattice L, we have:

$$\prod_{i \leq n} \lambda_i(L) \leq \sqrt{n}^n \cdot \det(L).$$

Minkowski's theorems

Provides a relationship between the invariants we have seen so far.

Minkowski's theorem

Let $L \subseteq \mathbb{R}^n$ be a full-rank lattice and $S \subseteq \mathbb{R}^n$ convex and symmetric with $\mathrm{vol}(S) > 2^n \cdot \det(L)$. Then there is $x \in (L \setminus 0) \cap S$. If S is closed, it suffices that $\mathrm{vol}(S) \geq 2^n \cdot \det(L)$.

Corollary 1

For any n-dimensional lattice L, we have: $\lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

Corollary 2

For any n-dimensional lattice L, we have:

$$\prod_{i \leq n} \lambda_i(L) \leq \sqrt{n}^n \cdot \det(L).$$

Hermite's constants

Minkowski's theorem implies the existence of Hermite's constant:

$$\gamma_n = \sup \left(\frac{\lambda_1(L)}{\det(L)^{1/n}} : \dim(L) = n \right)^2 .$$

For most n's, only bounds of γ_n are known. Known values:

n	2	3	4	5	6	7	8	24
γ_n^n	$4/3$	2	4	8	$64/3$	64	256	4^{24}

The Gaussian heuristic

The Gaussian heuristic

Given a full-dim lattice L and a 'nice' set S, the number of points of L within S is expected to be $\mathrm{vol}(S)/\det(L)$.

- Can be made rigorous for fixed lattice and growing S.
- Can be made rigorous for 'random' lattices L.
- Allows one to quickly estimate the number of points in a body.

The Gaussian heuristic

The Gaussian heuristic

Given a full-dim lattice L and a 'nice' set S, the number of points of L within S is expected to be $\mathrm{vol}(S)/\det(L)$.

- Can be made rigorous for fixed lattice and growing S.
- Can be made rigorous for 'random' lattices L.
- Allows one to quickly estimate the number of points in a body.

The Gaussian heuristic

The Gaussian heuristic

Given a full-dim lattice L and a 'nice' set S, the number of points of L within S is expected to be $\mathrm{vol}(S)/\det(L)$.

- Can be made rigorous for fixed lattice and growing S.
- Can be made rigorous for 'random' lattices L.
- Allows one to quickly estimate the number of points in a body.

The Gaussian heuristic

The Gaussian heuristic

Given a full-dim lattice L and a 'nice' set S, the number of points of L within S is expected to be $\mathrm{vol}(S)/\det(L)$.

- Can be made rigorous for fixed lattice and growing S.
- Can be made rigorous for 'random' lattices L.
- Allows one to quickly estimate the number of points in a body.

Outline

1. Lattices and lattice bases.
2. Lattice invariants.
3. **Examples of lattices.**
4. Gram-Schmidt orthogonalisation.
5. Lattice Gaussians.
6. Computational problems on lattices.

From linear codes to lattices

- A linear code C over $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime is a sub-vector space of a $\mathbb{Z}_p^n$.
- There exists a generator matrix $G \in \mathbb{Z}_p^{n \times k}$ with $k = \dim C$ s.t.:

$$C = G \cdot \mathbb{Z}_p^k = \{G\mathbf{s} : \mathbf{s} \in \mathbb{Z}_p^k\}.$$

Construction A

Let $C \subseteq \mathbb{Z}_p^n$ be a k-dimensional linear code.
The construction A lattice associated to C is:

$$L(C) = C + p\mathbb{Z}^n = \left\{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_p^k,\ \mathbf{x} = G \cdot \mathbf{s} \bmod p\right\}.$$

From linear codes to lattices

- A linear code C over $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime is a sub-vector space of a $\mathbb{Z}_p^n$.
- There exists a generator matrix $G \in \mathbb{Z}_p^{n \times k}$ with $k = \dim C$ s.t.:

$$C = G \cdot \mathbb{Z}_p^k = \{G\mathbf{s} : \mathbf{s} \in \mathbb{Z}_p^k\}.$$

Construction A

Let $C \subseteq \mathbb{Z}_p^n$ be a k-dimensional linear code.
The construction A lattice associated to C is:

$$L(C) = C + p\mathbb{Z}^n = \left\{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_p^k,\ \mathbf{x} = G \cdot \mathbf{s} \bmod p\right\}.$$

From linear codes to lattices

$$L(C) = C + p\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_p^k,\ \mathbf{x} = G \cdot \mathbf{s} \bmod p\}.$$

Simple properties:

- $p\mathbb{Z}^n \subseteq L(C) \subseteq \mathbb{Z}^n$. In particular, $\dim(L(C)) = n$.
- A basis of $L(C)$ is obtained using the HNF of $[G|p \cdot Id_n]$.

Determinant:

- As $L(A) \subseteq \mathbb{Z}^n$ is full-rank, it suffices to compute $|\mathbb{Z}^n/L(C)|$.
- As $\mathbb{Z}^n/L(C) \cong \mathbb{Z}_p^n/C$, we get: $\det(L(C)) = p^{n-k}$.

Minimum: by Minkowski's theorem, $\lambda_1(L(C)) \leq \sqrt{n} \cdot p^{1-k/n}$.

Dual: $\widehat{L(C)} = \frac{1}{p} \cdot L(C^\perp)$, with $C^\perp = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x}^T \cdot C = \mathbf{0}\}$.

From linear codes to lattices

$$L(C) = C + p\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_p^k,\ \mathbf{x} = G \cdot \mathbf{s} \bmod p\}.$$

Simple properties:

- $p\mathbb{Z}^n \subseteq L(C) \subseteq \mathbb{Z}^n$. In particular, $\dim(L(C)) = n$.
- A basis of $L(C)$ is obtained using the HNF of $[G|p \cdot Id_n]$.

Determinant:

- As $L(A) \subseteq \mathbb{Z}^n$ is full-rank, it suffices to compute $|\mathbb{Z}^n/L(C)|$.
- As $\mathbb{Z}^n/L(C) \cong \mathbb{Z}_p^n/C$, we get: $\det(L(C)) = p^{n-k}$.

Minimum: by Minkowski's theorem, $\lambda_1(L(C)) \leq \sqrt{n} \cdot p^{1-k/n}$.

Dual: $\widehat{L(C)} = \frac{1}{p} \cdot L(C^\perp)$, with $C^\perp = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x}^T \cdot C = \mathbf{0}\}$.

From linear codes to lattices

$$L(C) = C + p\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_p^k,\ \mathbf{x} = G \cdot \mathbf{s} \bmod p\}.$$

Simple properties:

- $p\mathbb{Z}^n \subseteq L(C) \subseteq \mathbb{Z}^n$. In particular, $\dim(L(C)) = n$.
- A basis of $L(C)$ is obtained using the HNF of $[G|p \cdot Id_n]$.

Determinant:

- As $L(A) \subseteq \mathbb{Z}^n$ is full-rank, it suffices to compute $|\mathbb{Z}^n/L(C)|$.
- As $\mathbb{Z}^n/L(C) \cong \mathbb{Z}_p^n/C$, we get: $\det(L(C)) = p^{n-k}$.

Minimum: by Minkowski's theorem, $\lambda_1(L(C)) \leq \sqrt{n} \cdot p^{1-k/n}$.

Dual: $\widehat{L(C)} = \frac{1}{p} \cdot L(C^\perp)$, with $C^\perp = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x}^T \cdot C = \mathbf{0}\}$.

From linear codes to lattices

$$L(C) = C + p\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_p^k,\ \mathbf{x} = G \cdot \mathbf{s} \bmod p\}.$$

Simple properties:

- $p\mathbb{Z}^n \subseteq L(C) \subseteq \mathbb{Z}^n$. In particular, $\dim(L(C)) = n$.
- A basis of $L(C)$ is obtained using the HNF of $[G|p \cdot Id_n]$.

Determinant:

- As $L(A) \subseteq \mathbb{Z}^n$ is full-rank, it suffices to compute $|\mathbb{Z}^n/L(C)|$.
- As $\mathbb{Z}^n/L(C) \cong \mathbb{Z}_p^n/C$, we get: $\det(L(C)) = p^{n-k}$.

Minimum: by Minkowski's theorem, $\lambda_1(L(C)) \leq \sqrt{n} \cdot p^{1-k/n}$.

Dual: $\widehat{L(C)} = \frac{1}{p} \cdot L(C^\perp)$, with $C^\perp = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x}^T \cdot C = \mathbf{0}\}$.

Construction A lattices in cryptography

Sample $A \in \mathbb{Z}_p^{m \times n}$ uniformly with $m > n$. We define:

- The LWE lattice of A as

$$\Lambda_p(A) = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_p^n : \mathbf{x} = A\mathbf{s} \bmod p\}.$$

$\Rightarrow$ Construction A on the code spanned by the columns of A.

- The SIS lattice of A as

$$\Lambda_p^{\perp}(A) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T A = \mathbf{0} \bmod p\}.$$

$\Rightarrow$ Construction A on the orthogonal of the latter code.

With overwhelming probability:

$$\det(\Lambda_p(A)) = p^{m-n} \quad \text{and} \quad \det(\Lambda_p^{\perp}(A)) = p^n.$$

Construction A lattices in cryptography

Sample $A \in \mathbb{Z}_p^{m \times n}$ uniformly with $m > n$. We define:

- The LWE lattice of A as

$$\Lambda_p(A) = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_p^n : \mathbf{x} = A\mathbf{s} \bmod p\}.$$

$\Rightarrow$ Construction A on the code spanned by the columns of A.

- The SIS lattice of A as

$$\Lambda_p^{\perp}(A) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T A = \mathbf{0} \bmod p\}.$$

$\Rightarrow$ Construction A on the orthogonal of the latter code.

With overwhelming probability:

$$\det(\Lambda_p(A)) = p^{m-n} \quad \text{and} \quad \det(\Lambda_p^{\perp}(A)) = p^n.$$

Construction A lattices in cryptography

Sample $A \in \mathbb{Z}_p^{m \times n}$ uniformly with $m > n$. We define:

- The LWE lattice of A as

$$\Lambda_p(A) = \{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}_p^n : \mathbf{x} = A\mathbf{s} \bmod p\}.$$

$\Rightarrow$ Construction A on the code spanned by the columns of A.

- The SIS lattice of A as

$$\Lambda_p^{\perp}(A) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T A = \mathbf{0} \bmod p\}.$$

$\Rightarrow$ Construction A on the orthogonal of the latter code.

With overwhelming probability:

$$\det(\Lambda_p(A)) = p^{m-n} \quad \text{and} \quad \det(\Lambda_p^{\perp}(A)) = p^n.$$

Lattices from integer matrices

Sample $A \in \mathbb{Z}^{m \times n}$ randomly, with $m > n$.

- $\{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x}^T \cdot A = \mathbf{0}\} = \ker_{\mathbb{Z}}(A) = \mathbb{Z}^m \cap \ker(A)$ is a lattice.
- Its dimension is $m - rk(A)$.
- Its determinant is harder to compute : $-$).

- Used in cryptanalysis (against knapsack-based cryptosystems).
- Recently used in cryptographic design (see [AgrGenHalSah13]).

Lattices from integer matrices

Sample $A \in \mathbb{Z}^{m \times n}$ randomly, with $m > n$.

- $\{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x}^T \cdot A = \mathbf{0}\} = \ker_{\mathbb{Z}}(A) = \mathbb{Z}^m \cap \ker(A)$ is a lattice.
- Its dimension is $m - rk(A)$.
- Its determinant is harder to compute : $-$).

- Used in cryptanalysis (against knapsack-based cryptosystems).
- Recently used in cryptographic design (see [AgrGenHalSah13]).

Ideal lattices

A lattice $L \subseteq \mathbb{Z}^n$ is ideal if $\forall (b_0 b_1 \ldots b_{n-1}) \in \mathbb{Z}^n$:

$$\begin{array}{rcccccccc} & (& b_0 & b_1 & b_2 & \ldots & b_{n-1} &) & \in L \\ \Rightarrow & (& -b_{n-1} & b_0 & b_1 & \ldots & b_{n-2} &) & \in L \\ \Rightarrow & (& -b_{n-2} & -b_{n-1} & b_0 & \ldots & b_{n-3} &) & \in L \end{array}$$

By identifying $\mathbb{Z}^n$ with $\mathbb{Z}[x]/(x^n+1)$, we obtain that:

L is ideal iff it corresponds to an ideal of $\mathbb{Z}[x]/(x^n+1)$.

If n is a power of 2, then $\det(L)^{1/n} \leq \lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

Ideal lattices

A lattice $L \subseteq \mathbb{Z}^n$ is ideal if $\forall (b_0 b_1 \ldots b_{n-1}) \in \mathbb{Z}^n$:

$$
\begin{array}{rcccccccl}
 & (& b_0 & b_1 & b_2 & \ldots & b_{n-1} &) & \in L \\
\Rightarrow & (& -b_{n-1} & b_0 & b_1 & \ldots & b_{n-2} &) & \in L \\
\Rightarrow & (& -b_{n-2} & -b_{n-1} & b_0 & \ldots & b_{n-3} &) & \in L
\end{array}
$$

By identifying $\mathbb{Z}^n$ with $\mathbb{Z}[x]/(x^n+1)$, we obtain that:

L is ideal iff it corresponds to an ideal of $\mathbb{Z}[x]/(x^n+1)$.

If n is a power of 2, then $\det(L)^{1/n} \leq \lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

- Consider the shifts $\mathbf{b}_i$ of a vector reaching $\lambda_1(L)$.
- As x^n+1 is irreducible, $L' = \sum \mathbb{Z}\mathbf{b}_i \subseteq L$ is full-rank.
- We have $\det(L) \leq \det(L') \leq \prod_i \|\mathbf{b}_i\| = \lambda_1(L)^n$.

Ideal lattices

A lattice $L \subseteq \mathbb{Z}^n$ is ideal if $\forall (b_0 b_1 \ldots b_{n-1}) \in \mathbb{Z}^n$:

$$\begin{array}{cccccccc} & (& b_0 & b_1 & b_2 & \ldots & b_{n-1} &) \in L \\ \Rightarrow & (& -b_{n-1} & b_0 & b_1 & \ldots & b_{n-2} &) \in L \\ \Rightarrow & (& -b_{n-2} & -b_{n-1} & b_0 & \ldots & b_{n-3} &) \in L \end{array}$$

By identifying $\mathbb{Z}^n$ with $\mathbb{Z}[x]/(x^n+1)$, we obtain that:

L is ideal iff it corresponds to an ideal of $\mathbb{Z}[x]/(x^n+1)$.

If n is a power of 2, then $\det(L)^{1/n} \leq \lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

- Consider the shifts $\mathbf{b}_i$ of a vector reaching $\lambda_1(L)$.
- As x^n+1 is irreducible, $L' = \sum \mathbb{Z}\mathbf{b}_i \subseteq L$ is full-rank.
- We have $\det(L) \leq \det(L') \leq \prod_i \|\mathbf{b}_i\| = \lambda_1(L)^n$.

Ideal lattices

A lattice $L \subseteq \mathbb{Z}^n$ is ideal if $\forall (b_0 b_1 \ldots b_{n-1}) \in \mathbb{Z}^n$:

$$\begin{array}{cccccccc} & (& b_0 & b_1 & b_2 & \ldots & b_{n-1} &) & \in L \\ \Rightarrow & (& -b_{n-1} & b_0 & b_1 & \ldots & b_{n-2} &) & \in L \\ \Rightarrow & (& -b_{n-2} & -b_{n-1} & b_0 & \ldots & b_{n-3} &) & \in L \end{array}$$

By identifying $\mathbb{Z}^n$ with $\mathbb{Z}[x]/(x^n+1)$, we obtain that:

L is ideal iff it corresponds to an ideal of $\mathbb{Z}[x]/(x^n+1)$.

If n is a power of 2, then $\det(L)^{1/n} \leq \lambda_1(L) \leq \sqrt{n} \cdot \det(L)^{1/n}$.

- Consider the shifts $\mathbf{b}_i$ of a vector reaching $\lambda_1(L)$.
- As x^n+1 is irreducible, $L' = \sum \mathbb{Z}\mathbf{b}_i \subseteq L$ is full-rank.
- We have $\det(L) \leq \det(L') \leq \prod_i \|\mathbf{b}_i\| = \lambda_1(L)^n$.

Ideal lattices and algebraic number theory

Let ζ be an algebraic integer, with minimal polynomial $P(x)$.

- The number field $K = \mathbb{Q}(\zeta)$ is isomorphic to $\mathbb{Q}[x]/P(x)$.
- The ring of integers $\mathcal{O}_K$ is the set of algebraic integers of K.

Let $(\zeta_i)_{i \leq r}$ be the real roots of P, and $(\zeta_{r+i})_{i \leq 2s}$ be its complex roots with $\zeta_{r+s+i} = \overline{\zeta_{r+i}}$.

- The embeddings σ_i of K are induced by $x \mapsto \zeta_i$.
- For $\alpha \in K$, set $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$.

Lattices from $\mathcal{O}_K$:

- For any ideal I of $\mathcal{O}_K$, $\sigma(I)$ is a lattice of $\mathbb{R}^n$.
- The lattices of the previous slide are isometric to the $\sigma(I)$'s, for $\zeta = \exp(i\pi/n)$ (with n a power of 2).
- In that case, $P = x^n + 1$ and $\mathcal{O}_K \cong \mathbb{Z}[x]/(x^n + 1)$.

Ideal lattices and algebraic number theory

Let ζ be an algebraic integer, with minimal polynomial $P(x)$.

- The number field $K = \mathbb{Q}(\zeta)$ is isomorphic to $\mathbb{Q}[x]/P(x)$.
- The ring of integers $\mathcal{O}_K$ is the set of algebraic integers of K.

Let $(\zeta_i)_{i \leq r}$ be the real roots of P, and $(\zeta_{r+i})_{i \leq 2s}$ be its complex roots with $\zeta_{r+s+i} = \overline{\zeta_{r+i}}$.

- The embeddings σ_i of K are induced by $x \mapsto \zeta_i$.
- For $\alpha \in K$, set $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$.

Lattices from $\mathcal{O}_K$:

- For any ideal I of $\mathcal{O}_K$, $\sigma(I)$ is a lattice of $\mathbb{R}^n$.
- The lattices of the previous slide are isometric to the $\sigma(I)$'s, for $\zeta = \exp(i\pi/n)$ (with n a power of 2).
- In that case, $P = x^n + 1$ and $\mathcal{O}_K \cong \mathbb{Z}[x]/(x^n + 1)$.

Ideal lattices and algebraic number theory

Let ζ be an algebraic integer, with minimal polynomial $P(x)$.

- The number field $K = \mathbb{Q}(\zeta)$ is isomorphic to $\mathbb{Q}[x]/P(x)$.
- The ring of integers $\mathcal{O}_K$ is the set of algebraic integers of K.

Let $(\zeta_i)_{i \leq r}$ be the real roots of P, and $(\zeta_{r+i})_{i \leq 2s}$ be its complex roots with $\zeta_{r+s+i} = \overline{\zeta_{r+i}}$.

- The embeddings σ_i of K are induced by $x \mapsto \zeta_i$.
- For $\alpha \in K$, set $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$.

Lattices from $\mathcal{O}_K$:

- For any ideal I of $\mathcal{O}_K$, $\sigma(I)$ is a lattice of $\mathbb{R}^n$.
- The lattices of the previous slide are isometric to the $\sigma(I)$'s, for $\zeta = \exp(i\pi/n)$ (with n a power of 2).
- In that case, $P = x^n + 1$ and $\mathcal{O}_K \cong \mathbb{Z}[x]/(x^n + 1)$.

Ideal lattices and algebraic number theory

Let ζ be an algebraic integer, with minimal polynomial $P(x)$.

- The number field $K = \mathbb{Q}(\zeta)$ is isomorphic to $\mathbb{Q}[x]/P(x)$.
- The ring of integers $\mathcal{O}_K$ is the set of algebraic integers of K.

Let $(\zeta_i)_{i \leq r}$ be the real roots of P, and $(\zeta_{r+i})_{i \leq 2s}$ be its complex roots with $\zeta_{r+s+i} = \overline{\zeta_{r+i}}$.

- The embeddings σ_i of K are induced by $x \mapsto \zeta_i$.
- For $\alpha \in K$, set $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$.

Lattices from $\mathcal{O}_K$:

- For any ideal I of $\mathcal{O}_K$, $\sigma(I)$ is a lattice of $\mathbb{R}^n$.
- The lattices of the previous slide are isometric to the $\sigma(I)$'s, for $\zeta = \exp(i\pi/n)$ (with n a power of 2).
- In that case, $P = x^n + 1$ and $\mathcal{O}_K \cong \mathbb{Z}[x]/(x^n + 1)$.

Outline

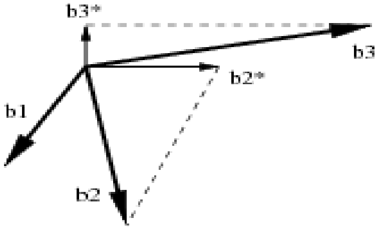
1. Lattices and lattice bases.
2. Lattice invariants.
3. Examples of lattices.
4. **Gram-Schmidt orthogonalisation.**
5. Lattice Gaussians.
6. Computational problems on lattices.

Gram-Schmidt Orthogonalisation

Gram-Schmidt orthogonalisation

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{R}^n$ be linearly independent. Their Gram-Schmidt orthogonalisation (GSO) is defined by:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*, \text{ with } \mu_{ij} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \text{ for all } i > j.$$



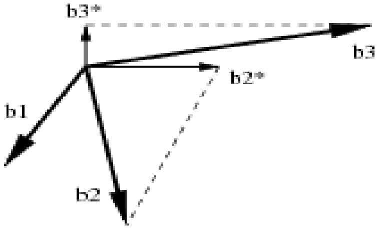
For all i, $\mathbf{b}_i^*$ is the projection of $\mathbf{b}_i$ orthogonally to $\sum_{j<i} \mathbb{R}\mathbf{b}_j$.

Gram-Schmidt Orthogonalisation

Gram-Schmidt orthogonalisation

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{R}^n$ be linearly independent. Their Gram-Schmidt orthogonalisation (GSO) is defined by:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*, \text{ with } \mu_{ij} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \text{ for all } i > j.$$



For all i, $\mathbf{b}_i^*$ is the projection of $\mathbf{b}_i$ orthogonally to $\sum_{j<i} \mathbb{R}\mathbf{b}_j$.

Properties of the GSO

- The μ_{ij}'s are unlikely to be integral, and so are unsuited for lattice basis transformations.
- For all i, we have $\sum_{j<i} \mathbb{R}\mathbf{b}_j^* = \sum_{j<i} \mathbb{R}\mathbf{b}_j$.
- The $\mathbf{b}_i^*$'s are orthogonal:

$$\|\mathbf{b}_i\|^2 = \|\mathbf{b}_i^*\|^2 + \sum_{j<i} \mu_{ij}^2 \|\mathbf{b}_j^*\|^2.$$

  In particular, $\|\mathbf{b}_i^*\| \leq \|\mathbf{b}_i\|$.
  We may attempt to make it sharper by lowering the μ_{ij}'s.

GSO and QR factorisation

QR factorisation

For any full-rank $B \in \mathbb{R}^{n \times n}$, there exists a unique pair of matrices $Q, R \in \mathbb{R}^{n \times n}$ such that:

- $B = Q \cdot R$;
- Q is orthogonal, i.e., $Q^T \cdot Q = Q \cdot Q^T = Id$;
- R is up-triangular with $r_{ii} > 0$ for all i.

QR and Gram-Schmidt encode the same information:

- $r_{ii} = \|\mathbf{b}_i^*\|$
- $r_{ij} = \mu_{ji} \cdot \|\mathbf{b}_i^*\|$
- $\mathbf{q}_i = \mathbf{b}_i^* / \|\mathbf{b}_i^*\|$.

GSO and QR factorisation

QR factorisation

For any full-rank $B \in \mathbb{R}^{n \times n}$, there exists a unique pair of matrices $Q, R \in \mathbb{R}^{n \times n}$ such that:

- $B = Q \cdot R$;
- Q is orthogonal, i.e., $Q^T \cdot Q = Q \cdot Q^T = Id$;
- R is up-triangular with $r_{ii} > 0$ for all i.

QR and Gram-Schmidt encode the same information:

- $r_{ii} = \|\mathbf{b}_i^*\|$
- $r_{ij} = \mu_{ji} \cdot \|\mathbf{b}_i^*\|$
- $\mathbf{q}_i = \mathbf{b}_i^* / \|\mathbf{b}_i^*\|$.

GSO and lattices

Minimum and GSO

Let L be a lattice, and $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of L. Then:

$$\lambda_1(L) \geq \min_j \|\mathbf{b}_j^*\|.$$

Determinant and GSO

Let L be a lattice, and $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of L. Then:

$$\det(L) = \prod_j \|\mathbf{b}_j^*\|.$$

Dual and GSO

Let $B \in \mathbb{R}^{n \times n}$ be non-singular, with factorisation $B = QR$. Then

$$(BJ)^{-T} = (QJ) \cdot (JR^{-T}J),$$

with J the mirror permutation matrix.

$\Rightarrow$ For any basis B, $\max_i \|\mathbf{b}_i^*\| = 1/\min_i \|\mathbf{c}_i^*\|$, where $C = \widehat{BJ}$.

GSO and lattices

Minimum and GSO

Let L be a lattice, and $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of L. Then:

$$\lambda_1(L) \geq \min_j \|\mathbf{b}_j^*\|.$$

Determinant and GSO

Let L be a lattice, and $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of L. Then:

$$\det(L) = \prod_j \|\mathbf{b}_j^*\|.$$

Dual and GSO

Let $B \in \mathbb{R}^{n \times n}$ be non-singular, with factorisation $B = QR$. Then

$$(BJ)^{-T} = (QJ) \cdot (JR^{-T}J),$$

with J the mirror permutation matrix.
$\Rightarrow$ For any basis B, $\max_i \|\mathbf{b}_i^*\| = 1/\min_i \|\mathbf{c}_i^*\|$, where $C = \widehat{BJ}$.

GSO and lattices

Minimum and GSO

Let L be a lattice, and $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of L. Then:

$$\lambda_1(L) \geq \min_j \|\mathbf{b}_j^*\|.$$

Determinant and GSO

Let L be a lattice, and $\mathbf{b}_1, \ldots, \mathbf{b}_d$ be a basis of L. Then:

$$\det(L) = \prod_j \|\mathbf{b}_j^*\|.$$

Dual and GSO

Let $B \in \mathbb{R}^{n \times n}$ be non-singular, with factorisation $B = QR$. Then

$$(BJ)^{-T} = (QJ) \cdot (JR^{-T}J),$$

with J the mirror permutation matrix.
$\Rightarrow$ For any basis B, $\max_i \|\mathbf{b}_i^*\| = 1/\min_i \|\mathbf{c}_i^*\|$, where $C = \widehat{BJ}$.

Size-reduction

Size-reduction aims at almost zeroing the μ_{ij}'s using integer ops.

Recall the GSO of a basis $(\mathbf{b}_i)_{i \leq d}$:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*, \text{ with } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \text{ for all } i > j.$$

Size-reducedness

A basis $(\mathbf{b}_i)_{i \leq d}$ is said size-reduced if $|\mu_{i,j}| \leq 1/2$ for all $i > j$.

Main property of size-reduced bases

If $(\mathbf{b}_i)_i$ is size-reduced, then

$$\|\mathbf{b}_i\|^2 \leq \|\mathbf{b}_i^*\|^2 + \frac{1}{4} \sum_{j<i} \|\mathbf{b}_j^*\|^2.$$

Size-reduction

Size-reduction aims at almost zeroing the μ_{ij}'s using integer ops.

Recall the GSO of a basis $(\mathbf{b}_i)_{i\leq d}$:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j}\mathbf{b}_j^*, \text{ with } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \text{ for all } i > j.$$

Size-reducedness

A basis $(\mathbf{b}_i)_{i\leq d}$ is said size-reduced if $|\mu_{i,j}| \leq 1/2$ for all $i > j$.

Main property of size-reduced bases

If $(\mathbf{b}_i)_i$ is size-reduced, then

$$\|\mathbf{b}_i\|^2 \leq \|\mathbf{b}_i^*\|^2 + \frac{1}{4}\sum_{j<i} \|\mathbf{b}_j^*\|^2.$$

Size-reduction

Size-reduction aims at almost zeroing the μ_{ij}'s using integer ops.

Recall the GSO of a basis $(\mathbf{b}_i)_{i \leq d}$:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*, \text{ with } \mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2} \text{ for all } i > j.$$

Size-reducedness

A basis $(\mathbf{b}_i)_{i \leq d}$ is said size-reduced if $|\mu_{i,j}| \leq 1/2$ for all $i > j$.

Main property of size-reduced bases

If $(\mathbf{b}_i)_i$ is size-reduced, then

$$\|\mathbf{b}_i\|^2 \leq \|\mathbf{b}_i^*\|^2 + \frac{1}{4} \sum_{j<i} \|\mathbf{b}_j^*\|^2.$$

The size-reduction algorithm

- Input: Basis $(\mathbf{b}_i)_{i \leq n}$ of a lattice L.
- Output: Size-reduced output $(\mathbf{c}_i)_{i \leq n}$ of L.

1. Compute the GSO coefficients μ_{ij}.
2. For all i, do:
3. For j from $i-1$ to 1, do:
4. $x_{ij} = \lfloor \mu_{ij} \rceil$.
5. $\mathbf{b}_i = \mathbf{b}_i - x_{ij}\mathbf{b}_j$.
6. For k from 1 to j do $\mu_{ik} = \mu_{ik} - x_{ij} \cdot \mu_{jk}$.

Also known as: Size-reduction, Babai's nearest plane algorithm, successive interference cancellation.

The size-reduction algorithm

- Input: Basis $(\mathbf{b}_i)_{i\leq n}$ of a lattice L.
- Output: Size-reduced output $(\mathbf{c}_i)_{i\leq n}$ of L.

1. Compute the GSO coefficients μ_{ij}.
2. For all i, do:
3. For j from $i-1$ to 1, do:
4. $x_{ij} = \lfloor \mu_{ij} \rceil$.
5. $\mathbf{b}_i = \mathbf{b}_i - x_{ij}\mathbf{b}_j$.
6. For k from 1 to j do $\mu_{ik} = \mu_{ik} - x_{ij} \cdot \mu_{jk}$.

Also known as: Size-reduction, Babai's nearest plane algorithm, successive interference cancellation.

Correctness and complexity

Correctness of the size-reduction algorithm

Let $(\mathbf{b}_i)_i$ be given as input to the size-reduction algorithm. Then the output is a size-reduced basis $(\mathbf{c}_i)_i$ of the same lattice. Furthermore:

1. For all i: $\mathbf{b}_i^* = \mathbf{c}_i^*$
2. For all i: $\|\mathbf{c}_i\| \leq \sqrt{n} \cdot \max_{j \leq i} \|\mathbf{b}_j^*\| \leq \sqrt{n} \cdot \max_{j \leq i} \|\mathbf{b}_j\|$
3. The corresponding unimodular transform is up-triangular with 1's on its diagonal.

If the $\mathbf{b}_i$'s are rational, then the bit-cost of the size-reduction algorithm is polynomial in the input size.

Correctness and complexity

Correctness of the size-reduction algorithm

Let $(\mathbf{b}_i)_i$ be given as input to the size-reduction algorithm. Then the output is a size-reduced basis $(\mathbf{c}_i)_i$ of the same lattice. Furthermore:

1. For all i: $\mathbf{b}_i^* = \mathbf{c}_i^*$
2. For all i: $\|\mathbf{c}_i\| \leq \sqrt{n} \cdot \max_{j \leq i} \|\mathbf{b}_j^*\| \leq \sqrt{n} \cdot \max_{j \leq i} \|\mathbf{b}_j\|$
3. The corresponding unimodular transform is up-triangular with 1's on its diagonal.

If the $\mathbf{b}_i$'s are rational, then the bit-cost of the size-reduction algorithm is polynomial in the input size.

From short vectors to a short basis

- Let $(\mathbf{b}_i)_i$ be an arbitrary basis of a lattice L.
- Let $(\mathbf{s}_i)_i$ in L be linearly independent with small $\|\mathbf{s}_i\|$'s.
- Can we compute a small basis of L?

1. Write $(\mathbf{s}_i)_i = (\mathbf{b}_i)_i \cdot T$, with $T \in \mathbb{Z}^{n\times n}$.
2. Compute the transpose-HNF of T, i.e.,
   $T = U \cdot H$ with $U \in \mathrm{GL}_n(\mathbb{Z})$ and $H \in \mathbb{Z}^{n\times n}$ up-triangular.
3. Let $(\mathbf{c}_i)_i = (\mathbf{b}_i)_i \cdot U$. It's a basis of L and $(\mathbf{s}_i)_i = (\mathbf{c}_i)_i \cdot H$.
   $$\max \|\mathbf{c}_i^*\| \leq \max \|\mathbf{s}_i^*\| \leq \max \|\mathbf{s}_i\|.$$
4. With a size-reduction, we get a basis $(\mathbf{d}_i)_i$ with
   $$\max \|\mathbf{d}_i\| \leq \sqrt{n} \cdot \max \|\mathbf{c}_i^*\| \leq \sqrt{n} \cdot \max \|\mathbf{s}_i\|.$$

From short vectors to a short basis

- Let $(\mathbf{b}_i)_i$ be an arbitrary basis of a lattice L.
- Let $(\mathbf{s}_i)_i$ in L be linearly independent with small $\|\mathbf{s}_i\|$'s.
- Can we compute a small basis of L?

1. Write $(\mathbf{s}_i)_i = (\mathbf{b}_i)_i \cdot T$, with $T \in \mathbb{Z}^{n \times n}$.
2. Compute the transpose-HNF of T, i.e.,
   $T = U \cdot H$ with $U \in \mathrm{GL}_n(\mathbb{Z})$ and $H \in \mathbb{Z}^{n \times n}$ up-triangular.
3. Let $(\mathbf{c}_i)_i = (\mathbf{b}_i)_i \cdot U$. It's a basis of L and $(\mathbf{s}_i)_i = (\mathbf{c}_i)_i \cdot H$.
   $$\max \|\mathbf{c}_i^*\| \leq \max \|\mathbf{s}_i^*\| \leq \max \|\mathbf{s}_i\|.$$
4. With a size-reduction, we get a basis $(\mathbf{d}_i)_i$ with
   $$\max \|\mathbf{d}_i\| \leq \sqrt{n} \cdot \max \|\mathbf{c}_i^*\| \leq \sqrt{n} \cdot \max \|\mathbf{s}_i\|.$$

From short vectors to a short basis

- Let $(\mathbf{b}_i)_i$ be an arbitrary basis of a lattice L.
- Let $(\mathbf{s}_i)_i$ in L be linearly independent with small $\|\mathbf{s}_i\|$'s.
- Can we compute a small basis of L?

1. Write $(\mathbf{s}_i)_i = (\mathbf{b}_i)_i \cdot T$, with $T \in \mathbb{Z}^{n\times n}$.
2. Compute the transpose-HNF of T, i.e.,
   $T = U \cdot H$ with $U \in \mathrm{GL}_n(\mathbb{Z})$ and $H \in \mathbb{Z}^{n\times n}$ up-triangular.
3. Let $(\mathbf{c}_i)_i = (\mathbf{b}_i)_i \cdot U$. It's a basis of L and $(\mathbf{s}_i)_i = (\mathbf{c}_i)_i \cdot H$.
   $$\max \|\mathbf{c}_i^*\| \leq \max \|\mathbf{s}_i^*\| \leq \max \|\mathbf{s}_i\|.$$
4. With a size-reduction, we get a basis $(\mathbf{d}_i)_i$ with
   $$\max \|\mathbf{d}_i\| \leq \sqrt{n} \cdot \max \|\mathbf{c}_i^*\| \leq \sqrt{n} \cdot \max \|\mathbf{s}_i\|.$$

From short vectors to a short basis

- Let $(\mathbf{b}_i)_i$ be an arbitrary basis of a lattice L.
- Let $(\mathbf{s}_i)_i$ in L be linearly independent with small $\|\mathbf{s}_i\|$'s.
- Can we compute a small basis of L?

1. Write $(\mathbf{s}_i)_i = (\mathbf{b}_i)_i \cdot T$, with $T \in \mathbb{Z}^{n\times n}$.
2. Compute the transpose-HNF of T, i.e.,
   $T = U \cdot H$ with $U \in \mathrm{GL}_n(\mathbb{Z})$ and $H \in \mathbb{Z}^{n\times n}$ up-triangular.
3. Let $(\mathbf{c}_i)_i = (\mathbf{b}_i)_i \cdot U$. It's a basis of L and $(\mathbf{s}_i)_i = (\mathbf{c}_i)_i \cdot H$.
   $$\max \|\mathbf{c}_i^*\| \le \max \|\mathbf{s}_i^*\| \le \max \|\mathbf{s}_i\|.$$
4. With a size-reduction, we get a basis $(\mathbf{d}_i)_i$ with
   $$\max \|\mathbf{d}_i\| \le \sqrt{n} \cdot \max \|\mathbf{c}_i^*\| \le \sqrt{n} \cdot \max \|\mathbf{s}_i\|.$$

From short vectors to a short basis

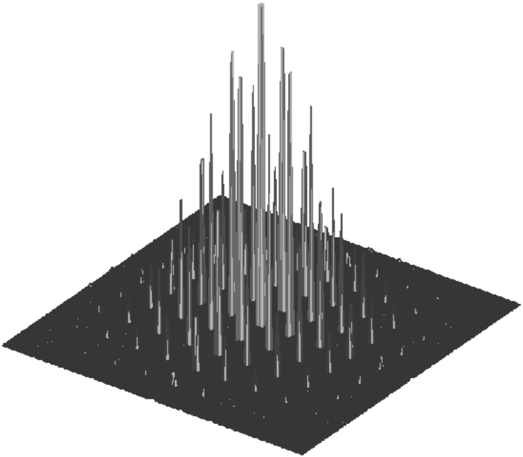
- Let $(\mathbf{b}_i)_i$ be an arbitrary basis of a lattice L.
- Let $(\mathbf{s}_i)_i$ in L be linearly independent with small $\|\mathbf{s}_i\|$'s.
- Can we compute a small basis of L?

1. Write $(\mathbf{s}_i)_i = (\mathbf{b}_i)_i \cdot T$, with $T \in \mathbb{Z}^{n \times n}$.
2. Compute the transpose-HNF of T, i.e.,
   $T = U \cdot H$ with $U \in \mathrm{GL}_n(\mathbb{Z})$ and $H \in \mathbb{Z}^{n \times n}$ up-triangular.
3. Let $(\mathbf{c}_i)_i = (\mathbf{b}_i)_i \cdot U$. It's a basis of L and $(\mathbf{s}_i)_i = (\mathbf{c}_i)_i \cdot H$.
   $$\max \|\mathbf{c}_i^*\| \leq \max \|\mathbf{s}_i^*\| \leq \max \|\mathbf{s}_i\|.$$
4. With a size-reduction, we get a basis $(\mathbf{d}_i)_i$ with
   $$\max \|\mathbf{d}_i\| \leq \sqrt{n} \cdot \max \|\mathbf{c}_i^*\| \leq \sqrt{n} \cdot \max \|\mathbf{s}_i\|.$$

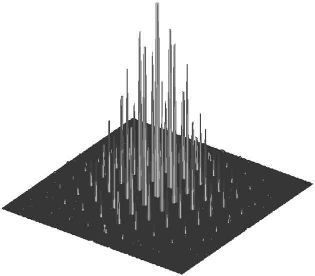
Outline

1. Lattices and lattice bases.
2. Lattice invariants.
3. Examples of lattices.
4. Gram-Schmidt orthogonalisation.
5. **Lattice Gaussians.**
6. Computational problems on lattices.

Lattice Gaussian distribution



Lattice Gaussian distribution

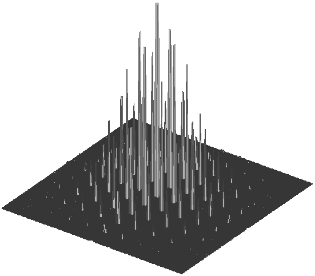


For $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{c} \in \mathbb{R}^n$:

$$\rho_{\sigma,\mathbf{c}}(\mathbf{b}) := \exp\left(-\pi \frac{\|\mathbf{b}-\mathbf{c}\|^2}{\sigma^2}\right).$$

σ is the standard deviation parameter.

Lattice Gaussian distribution



For $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{c} \in \mathbb{R}^n$:

$$\rho_{\sigma,\mathbf{c}}(\mathbf{b}) := \exp\left(-\pi \frac{\|\mathbf{b}-\mathbf{c}\|^2}{\sigma^2}\right).$$

σ is the standard deviation parameter.

For $L \subseteq \mathbb{R}^n$ and $\mathbf{c} \in \mathbb{R}^n$: $\rho_{\sigma,\mathbf{c}}(L) = \sum_{\mathbf{b}\in L} \rho_{\sigma,\mathbf{c}}(\mathbf{b})$ is finite.

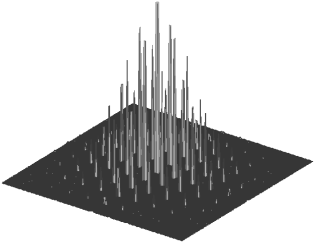
Gaussian distribution of support L and parameters $\mathbf{c}$ and σ

$$\forall \mathbf{b} \in L: \quad D_{L,\sigma,\mathbf{c}}(\mathbf{b}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{b})}{\rho_{\sigma,\mathbf{c}}(L)} \sim \rho_{\sigma,\mathbf{c}}(\mathbf{b}).$$

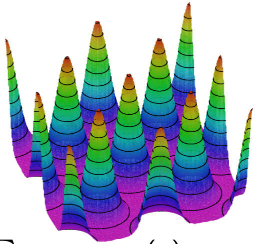
Fourier transform

$D_{L,\sigma,\mathbf{0}} \sim \rho_\sigma \cdot \mathbf{1}_L$, with $\mathbf{1}_L$ the indicator function of L.

- The Fourier transform of ρ_σ is $\rho_{\sigma^{-1}}$.
- The Fourier transform of $\mathbf{1}_L$ is $\mathbf{1}_{\widehat{L}}$.



$\mathbf{x} \mapsto D_{L,\sigma,\mathbf{0}}(\mathbf{x})$



$\mathbf{x} \mapsto \sum_{\widehat{\mathbf{b}} \in \widehat{L}} \rho_{\sigma^{-1},\widehat{\mathbf{b}}}(\mathbf{x}) = \rho_{\sigma^{-1},\mathbf{x}}(\widehat{L})$

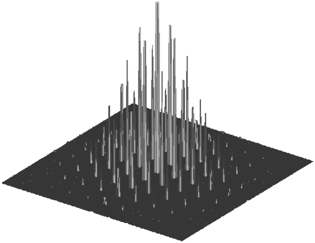
Poisson Summation Formula

$$\rho_{\sigma,\mathbf{c}}(L) = \sum_{\mathbf{b} \in L} \rho_{\sigma,\mathbf{c}}(\mathbf{b}) = \frac{\sigma^n}{\det L} \cdot \sum_{\widehat{\mathbf{b}} \in \widehat{L}} \rho_{\sigma^{-1}}(\widehat{\mathbf{b}}) \cdot e^{-2i\pi\langle \widehat{\mathbf{b}}, \mathbf{c}\rangle}.$$

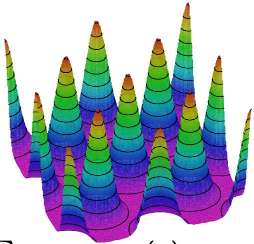
Fourier transform

$D_{L,\sigma,\mathbf{0}} \sim \rho_\sigma \cdot \mathbf{1}_L$, with $\mathbf{1}_L$ the indicator function of L.

- The Fourier transform of ρ_σ is $\rho_{\sigma^{-1}}$.
- The Fourier transform of $\mathbf{1}_L$ is $\mathbf{1}_{\widehat{L}}$.



$\mathbf{x} \mapsto D_{L,\sigma,\mathbf{0}}(\mathbf{x})$



$\mathbf{x} \mapsto \sum_{\widehat{\mathbf{b}} \in \widehat{L}} \rho_{\sigma^{-1},\widehat{\mathbf{b}}}(\mathbf{x}) = \rho_{\sigma^{-1},\mathbf{x}}(\widehat{L})$

Poisson Summation Formula

$$\rho_{\sigma,\mathbf{c}}(L) = \sum_{\mathbf{b}\in L} \rho_{\sigma,\mathbf{c}}(\mathbf{b}) = \frac{\sigma^n}{\det L} \cdot \sum_{\widehat{\mathbf{b}} \in \widehat{L}} \rho_{\sigma^{-1}}(\widehat{\mathbf{b}}) \cdot e^{-2i\pi\langle \hat{\mathbf{b}},\mathbf{c}\rangle}.$$

The smoothing parameter

It quantifies when σ is sufficiently large for:

- the distribution $D_{L,\mathbf{c},\sigma}$ to look smooth.
- the function $\mathbf{x} \mapsto \rho_{\sigma,\mathbf{x}}(L)$ to look constant.

Smoothing parameter

For $\varepsilon \in (0,1)$ and L a full-rank lattice, we define:

$$\eta_\varepsilon(L) \;=\; \min\left(\sigma : \rho_{\sigma^{-1},\mathbf{0}}(\hat{L} \setminus \mathbf{0}) \leq \varepsilon\right).$$

Flatness of $\mathbf{x} \mapsto \rho_{\sigma,\mathbf{x}}(L)$ for $\sigma \geq \eta_\varepsilon(L)$:

Consequence of the PSF:
$\rho_{\sigma,\mathbf{x}}(L) = \frac{\sigma^n}{\det L} \cdot \sum_{\hat{\mathbf{b}} \in \hat{L}} \rho_{\sigma^{-1},\mathbf{0}}(\hat{\mathbf{b}}) \cdot e^{-2i\pi\langle \hat{\mathbf{b}}, \mathbf{c}\rangle}$.

$$\left|\rho_{\sigma,\mathbf{x}}(L) - \frac{\sigma^n}{\det L}\right| \;\leq\; \frac{\sigma^n}{\det L} \cdot \sum_{\widehat{\mathbf{b}} \in \widehat{L} \setminus \mathbf{0}} \rho_{\sigma^{-1},\mathbf{0}}(\widehat{\mathbf{b}}) \;\leq\; \frac{\sigma^n}{\det L} \cdot \varepsilon.$$

The smoothing parameter

It quantifies when σ is sufficiently large for:

- the distribution $D_{L,\mathbf{c},\sigma}$ to look smooth.
- the function $\mathbf{x} \mapsto \rho_{\sigma,\mathbf{x}}(L)$ to look constant.

Smoothing parameter

For $\varepsilon \in (0,1)$ and L a full-rank lattice, we define:

$$\eta_\varepsilon(L) \; = \; \min\left(\sigma : \rho_{\sigma^{-1},\mathbf{0}}(\hat{L} \setminus \mathbf{0}) \leq \varepsilon\right).$$

Flatness of $\mathbf{x} \mapsto \rho_{\sigma,\mathbf{x}}(L)$ for $\sigma \geq \eta_\varepsilon(L)$:

Consequence of the PSF:
$\rho_{\sigma,\mathbf{x}}(L) = \frac{\sigma^n}{\det L} \cdot \sum_{\hat{\mathbf{b}} \in \hat{L}} \rho_{\sigma^{-1},\mathbf{0}}(\hat{\mathbf{b}}) \cdot e^{-2i\pi\langle \hat{\mathbf{b}},\mathbf{c}\rangle}$.

$$\left|\rho_{\sigma,\mathbf{x}}(L) - \frac{\sigma^n}{\det L}\right| \; \leq \; \frac{\sigma^n}{\det L} \cdot \sum_{\widehat{\mathbf{b}} \in \widehat{L} \setminus \mathbf{0}} \rho_{\sigma^{-1},\mathbf{0}}(\widehat{\mathbf{b}}) \; \leq \; \frac{\sigma^n}{\det L} \cdot \varepsilon.$$

The smoothing parameter

It quantifies when σ is sufficiently large for:

- the distribution $D_{L,\mathbf{c},\sigma}$ to look smooth.
- the function $\mathbf{x} \mapsto \rho_{\sigma,\mathbf{x}}(L)$ to look constant.

Smoothing parameter

For $\varepsilon \in (0,1)$ and L a full-rank lattice, we define:

$$\eta_\varepsilon(L) \;=\; \min\left(\sigma : \rho_{\sigma^{-1},\mathbf{0}}(\hat{L} \setminus \mathbf{0}) \leq \varepsilon\right).$$

Flatness of $\mathbf{x} \mapsto \rho_{\sigma,\mathbf{x}}(L)$ for $\sigma \geq \eta_\varepsilon(L)$:

Consequence of the PSF:
$\rho_{\sigma,\mathbf{x}}(L) = \frac{\sigma^n}{\det L} \cdot \sum_{\hat{\mathbf{b}} \in \hat{L}} \rho_{\sigma^{-1},\mathbf{0}}(\hat{\mathbf{b}}) \cdot e^{-2i\pi\langle \hat{\mathbf{b}},\mathbf{c}\rangle}$.

$$\left|\rho_{\sigma,\mathbf{x}}(L) - \frac{\sigma^n}{\det L}\right| \;\leq\; \frac{\sigma^n}{\det L} \cdot \sum_{\widehat{\mathbf{b}} \in \widehat{L} \setminus \mathbf{0}} \rho_{\sigma^{-1},\mathbf{0}}(\widehat{\mathbf{b}}) \;\leq\; \frac{\sigma^n}{\det L} \cdot \varepsilon.$$

Bounding the smoothing parameter

$$\eta_{2^{-n}}(L) \;\leq\; \sqrt{n} \;/\; \lambda_1(\hat{L}).$$

Proof sketch: Take $\sigma = \lambda_1(\hat{L})/\sqrt{n}$ in

$$\rho_\sigma(\hat{L} \setminus \mathbf{0}) = \sum_{\widehat{\mathbf{b}} \in \widehat{L} \setminus \mathbf{0}} \exp\left(-n\pi \frac{\|\widehat{\mathbf{b}}\|^2}{\lambda_1(\widehat{L})^2}\right).$$

The summand is $2^{-\Theta(n)}$ for $\|\widehat{\mathbf{b}}\| \approx \lambda_1(\widehat{L})$, and drops fast with $\|\widehat{\mathbf{b}}\|$.

$$\eta_{2^{-n}}(L) \;\leq\; \sqrt{n} \;\cdot\; \lambda_n(L).$$

Proof: Transference.

$$\eta_{2^{-n}}(L) \leq \max \|\mathbf{b}_i^*\| \text{ for any basis } \mathbf{b}_i \text{ of } L.$$

Proof: Let $C = (BJ)^{-T}$ be the dual basis of BJ. Then

$$\lambda_1(\hat{L}) \geq \min \|\mathbf{c}_i^*\| = 1/\max \|\mathbf{b}_i^*\|.$$

Bounding the smoothing parameter

$$\eta_{2^{-n}}(L) \;\leq\; \sqrt{n} \;/\; \lambda_1(\hat{L}).$$

Proof sketch: Take $\sigma = \lambda_1(\hat{L})/\sqrt{n}$ in

$$\rho_\sigma(\hat{L} \setminus \mathbf{0}) = \sum_{\widehat{\mathbf{b}} \in \widehat{L} \setminus \mathbf{0}} \exp\left(-n\pi \frac{\|\widehat{\mathbf{b}}\|^2}{\lambda_1(\widehat{L})^2}\right).$$

The summand is $2^{-\Theta(n)}$ for $\|\widehat{\mathbf{b}}\| \approx \lambda_1(\widehat{L})$, and drops fast with $\|\widehat{\mathbf{b}}\|$.

$$\eta_{2^{-n}}(L) \;\leq\; \sqrt{n} \;\cdot\; \lambda_n(L).$$

Proof: Transference.

$$\eta_{2^{-n}}(L) \leq \max \|\mathbf{b}_i^*\| \text{ for any basis } \mathbf{b}_i \text{ of } L.$$

Proof: Let $C = (BJ)^{-T}$ be the dual basis of BJ. Then

$$\lambda_1(\hat{L}) \geq \min \|\mathbf{c}_i^*\| = 1/\max \|\mathbf{b}_i^*\|.$$

Bounding the smoothing parameter

$$\eta_{2^{-n}}(L) \ \leq \ \sqrt{n} \ / \ \lambda_1(\hat{L}).$$

Proof sketch: Take $\sigma = \lambda_1(\hat{L})/\sqrt{n}$ in

$$\rho_\sigma(\hat{L} \setminus \mathbf{0}) = \sum_{\widehat{\mathbf{b}} \in \widehat{L} \setminus \mathbf{0}} \exp\left(-n\pi \frac{\|\widehat{\mathbf{b}}\|^2}{\lambda_1(\widehat{L})^2}\right).$$

The summand is $2^{-\Theta(n)}$ for $\|\widehat{\mathbf{b}}\| \approx \lambda_1(\widehat{L})$, and drops fast with $\|\widehat{\mathbf{b}}\|$.

$$\eta_{2^{-n}}(L) \ \leq \ \sqrt{n} \ \cdot \ \lambda_n(L).$$

Proof: Transference.

$$\eta_{2^{-n}}(L) \leq \max \|\mathbf{b}_i^*\| \text{ for any basis } \mathbf{b}_i \text{ of } L.$$

Proof: Let $C = (BJ)^{-T}$ be the dual basis of BJ. Then

$$\lambda_1(\hat{L}) \geq \min \|\mathbf{c}_i^*\| = 1/ \max \|\mathbf{b}_i^*\|.$$

Sampling from $D_{L,\sigma,\mathbf{c}}$

- Algorithm of [Klein'00], analyzed in [GenPeiVai'08].
- Randomized version of size-reduction.

Input: A basis $(\mathbf{b}_i)_i$ of L, σ.
Output: $\mathbf{b} \in L$, hopefully distributed from $D_{L,\sigma,\mathbf{0}}$.

1. $\mathbf{b} := \mathbf{0}$. For i from n to 1, do
2. $\sigma_i := \sigma/\|\mathbf{b}_i^*\|$, $c_i := -\langle \mathbf{b}, \mathbf{b}_i^* \rangle / \|\mathbf{b}_i^*\|^2$;
3. Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

It can be easily modified to sample according to $D_{L,\sigma,\mathbf{c}}$.

Sampling from $D_{L,\sigma,\mathbf{c}}$

- Algorithm of [Klein'00], analyzed in [GenPeiVai'08].
- Randomized version of size-reduction.

Input: A basis $(\mathbf{b}_i)_i$ of L, σ.
Output: $\mathbf{b} \in L$, hopefully distributed from $D_{L,\sigma,\mathbf{0}}$.

1. $\mathbf{b} := \mathbf{0}$. For i from n to 1, do
2. $\quad \sigma_i := \sigma/\|\mathbf{b}_i^*\|$, $c_i := -\langle \mathbf{b}, \mathbf{b}_i^* \rangle / \|\mathbf{b}_i^*\|^2$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

It can be easily modified to sample according to $D_{L,\sigma,\mathbf{c}}$.

Sampling from $D_{L,\sigma,\mathbf{c}}$

- Algorithm of [Klein'00], analyzed in [GenPeiVai'08].
- Randomized version of size-reduction.

Input: A basis $(\mathbf{b}_i)_i$ of L, σ.
Output: $\mathbf{b} \in L$, hopefully distributed from $D_{L,\sigma,\mathbf{0}}$.

1. $\mathbf{b} := \mathbf{0}$. For i from n to 1, do
2. $\quad \sigma_i := \sigma / \|\mathbf{b}_i^*\|$, $c_i := -\langle \mathbf{b}, \mathbf{b}_i^* \rangle / \|\mathbf{b}_i^*\|^2$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

It can be easily modified to sample according to $D_{L,\sigma,\mathbf{c}}$.

Sampling from $D_{L,\sigma,\mathbf{c}}$

- Algorithm of [Klein'00], analyzed in [GenPeiVai'08].
- Randomized version of size-reduction.

Input: A basis $(\mathbf{b}_i)_i$ of L, σ.
Output: $\mathbf{b} \in L$, hopefully distributed from $D_{L,\sigma,\mathbf{0}}$.

1. $\mathbf{b} := \mathbf{0}$. For i from n to 1, do
2. $\quad \sigma_i := \sigma/\|\mathbf{b}_i^*\|$, $c_i := -\langle \mathbf{b}, \mathbf{b}_i^* \rangle / \|\mathbf{b}_i^*\|^2$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

It can be easily modified to sample according to $D_{L,\sigma,\mathbf{c}}$.

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

The probability of returning $\mathbf{b} = \sum x_i \mathbf{b}_i$ is:

$\Pr[z_n = x_n] \cdot \Pr[z_{n-1} = x_{n-1} | z_n = x_n] \cdot \ldots \cdot \Pr[z_1 = x_1 | z_i = x_i, \forall i > 1]$.

Using the GSO, this is:

$$\prod D_{\mathbb{Z},\sigma_i,c_i}(x_i) = \frac{\exp(-\sum_i (x_i - c_i)^2/\sigma_i^2)}{\prod \rho_{\sigma_i,c_i}(\mathbb{Z})} = \frac{\exp(-\|\mathbf{b}\|^2/\sigma^2)}{\prod \rho_{\sigma_i,c_i}(\mathbb{Z})}.$$

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

The probability of returning $\mathbf{b} = \sum x_i \mathbf{b}_i$ is:

$$\Pr[z_n = x_n] \cdot \Pr[z_{n-1} = x_{n-1} | z_n = x_n] \cdot \ldots \cdot \Pr[z_1 = x_1 | z_i = x_i, \forall i > 1].$$

Using the GSO, this is:

$$\prod D_{\mathbb{Z},\sigma_i,c_i}(x_i) = \frac{\exp(-\sum_i (x_i - c_i)^2 / \sigma_i^2)}{\prod \rho_{\sigma_i,c_i}(\mathbb{Z})} = \frac{\exp(-\|\mathbf{b}\|^2 / \sigma^2)}{\prod \rho_{\sigma_i,c_i}(\mathbb{Z})}.$$

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

The probability of returning $\mathbf{b}$ is $\exp(-\|\mathbf{b}\|^2/\sigma^2) \;/\; \prod \rho_{\sigma_i,c_i}(\mathbb{Z})$.

- We'd like each $\rho_{\sigma_i,c_i}(\mathbb{Z})$ to be independent of $\mathbf{b}$.
- $\rho_{\sigma_i,c_i}(\mathbb{Z})$ is essentially independent of c_i when $\sigma_i \geq \eta_\varepsilon(\mathbb{Z})$.
- For $\varepsilon = 2^{-n}$, it suffices that $\forall i : \sigma/\|\mathbf{b}_i^*\| \geq \sqrt{n}$.

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

The probability of returning $\mathbf{b}$ is $\exp(-\|\mathbf{b}\|^2/\sigma^2) \ / \ \prod \rho_{\sigma_i,c_i}(\mathbb{Z})$.

- We'd like each $\rho_{\sigma_i,c_i}(\mathbb{Z})$ to be independent of $\mathbf{b}$.
- $\rho_{\sigma_i,c_i}(\mathbb{Z})$ is essentially independent of c_i when $\sigma_i \geq \eta_\varepsilon(\mathbb{Z})$.
- For $\varepsilon = 2^{-n}$, it suffices that $\forall i: \ \sigma/\|\mathbf{b}_i^*\| \ \geq \ \sqrt{n}$.

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

Sampling from a lattice Gaussian [GenPeiVai'08]

For $\sigma \geq \sqrt{n} \cdot \max \|\mathbf{b}_i^*\|$, Klein's algorithm samples from a distribution within statistical distance $\Delta = 2^{-\Omega(n)}$ to $D_{L,\sigma,\mathbf{c}}$.

- Stat. distance = total variation distance = L_1 distance.
- Algorithm $\mathcal{A}$ succeeds with prob. ε given a sample from D $\Rightarrow \mathcal{A}$ succeeds with prob. $\geq \varepsilon - \Delta$ given a sample from D'.
- We can get the exact distribution for $\sigma \geq 10\sqrt{\log n} \cdot \max \|\mathbf{b}_i^*\|$, using rejection sampling [BraLanPeiRegSte'13].

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

Sampling from a lattice Gaussian [GenPeiVai'08]

For $\sigma \geq \sqrt{n} \cdot \max \|\mathbf{b}_i^*\|$, Klein's algorithm samples from a distribution within statistical distance $\Delta = 2^{-\Omega(n)}$ to $D_{L,\sigma,\mathbf{c}}$.

- Stat. distance = total variation distance = L_1 distance.
- Algorithm $\mathcal{A}$ succeeds with prob. ε given a sample from D $\Rightarrow \mathcal{A}$ succeeds with prob. $\geq \varepsilon - \Delta$ given a sample from D'.
- We can get the exact distribution for $\sigma \geq 10\sqrt{\log n} \cdot \max \|\mathbf{b}_i^*\|$, using rejection sampling [BraLanPeiRegSte'13].

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

Sampling from a lattice Gaussian [GenPeiVai'08]

For $\sigma \geq \sqrt{n} \cdot \max \|\mathbf{b}_i^*\|$, Klein's algorithm samples from a distribution within statistical distance $\Delta = 2^{-\Omega(n)}$ to $D_{L,\sigma,\mathbf{c}}$.

- Stat. distance = total variation distance = L_1 distance.
- Algorithm $\mathcal{A}$ succeeds with prob. ε given a sample from D $\Rightarrow$ $\mathcal{A}$ succeeds with prob. $\geq \varepsilon - \Delta$ given a sample from D'.
- We can get the exact distribution for $\sigma \geq 10\sqrt{\log n} \cdot \max \|\mathbf{b}_i^*\|$, using rejection sampling [BraLanPeiRegSte'13].

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

Sampling from a lattice Gaussian [GenPeiVai'08]

For $\sigma \geq \sqrt{n} \cdot \max \|\mathbf{b}_i^*\|$, Klein's algorithm samples from a distribution within statistical distance $\Delta = 2^{-\Omega(n)}$ to $D_{L,\sigma,\mathbf{c}}$.

- Stat. distance = total variation distance = L_1 distance.
- Algorithm $\mathcal{A}$ succeeds with prob. ε given a sample from D $\Rightarrow$ $\mathcal{A}$ succeeds with prob. $\geq \varepsilon - \Delta$ given a sample from D'.
- We can get the exact distribution for $\sigma \geq 10\sqrt{\log n} \cdot \max \|\mathbf{b}_i^*\|$, using rejection sampling [BraLanPeiRegSte'13].

Sampling from $D_{L,\sigma,\mathbf{c}}$

1. $\mathbf{b} := \mathbf{0}$. For $i = n..1$, do:
2. $\quad \sigma_i := \frac{\sigma}{\|\mathbf{b}_i^*\|}$, $c_i := -\frac{\langle \mathbf{b}, \mathbf{b}_i^* \rangle}{\|\mathbf{b}_i^*\|^2}$;
3. $\quad$ Sample z_i from $D_{\mathbb{Z},\sigma_i,c_i}$;
4. $\quad \mathbf{b} := \mathbf{b} + z_i \mathbf{b}_i$.
5. Return $\mathbf{b}$.

Sampling from a lattice Gaussian [GenPeiVai'08]

For $\sigma \geq \sqrt{n} \cdot \max \|\mathbf{b}_i^*\|$, Klein's algorithm samples from a distribution within statistical distance $\Delta = 2^{-\Omega(n)}$ to $D_{L,\sigma,\mathbf{c}}$.

- Stat. distance = total variation distance = L_1 distance.
- Algorithm $\mathcal{A}$ succeeds with prob. ε given a sample from D $\Rightarrow \mathcal{A}$ succeeds with prob. $\geq \varepsilon - \Delta$ given a sample from D'.
- We can get the exact distribution for $\sigma \geq 10\sqrt{\log n} \cdot \max \|\mathbf{b}_i^*\|$, using rejection sampling [BraLanPeiRegSte'13].

Outline

1. Lattices and lattice bases.
2. Lattice invariants.
3. Examples of lattices.
4. Gram-Schmidt orthogonalisation.
5. Lattice Gaussians.
6. **Computational problems on lattices.**

Easy algorithmic problems on lattices

Given a basis of $L \subseteq \mathbb{Z}^n$, we can, in polynomial-time:

- Test whether a given $\mathbf{b}$ belongs to L
- Compute the determinant of L
- Compute a basis of $\widehat{L}$

Given a basis of $L_1 \subseteq \mathbb{Z}^n$ and a basis of $L_2 \subseteq \mathbb{Z}^n$, we can, in polynomial-time:

- Test whether $L_1 \subseteq L_2$.
- Test whether $L_1 = L_2$.
- Compute bases for $L_1 + L_2$ and $L_1 \cap L_2$.

Easy algorithmic problems on lattices

Given a basis of $L \subseteq \mathbb{Z}^n$, we can, in polynomial-time:

- Test whether a given $\mathbf{b}$ belongs to L
- Compute the determinant of L
- Compute a basis of $\widehat{L}$

Given a basis of $L_1 \subseteq \mathbb{Z}^n$ and a basis of $L_2 \subseteq \mathbb{Z}^n$, we can, in polynomial-time:

- Test whether $L_1 \subseteq L_2$.
- Test whether $L_1 = L_2$.
- Compute bases for $L_1 + L_2$ and $L_1 \cap L_2$.

The Shortest Vector Problem

It comes in many flavours, and can be generalized in many ways.

Computational SVP

Given a basis of L, find $\mathbf{b} \in L$ with $\|\mathbf{b}\| = \lambda_1(L)$.

Decisional SVP

Given a basis of L and a rational d, reply YES is $\lambda_1(L) \leq d$ and NO otherwise.

- We are mostly interested in SVP when the lattice dimension grows to infinity.
- [Van Emde Boas'81]: DecSVP is NP-hard for the infinity norm.
- [Ajtai'98]: DecSVP is NP-hard under randomized reductions.

The Shortest Vector Problem

It comes in many flavours, and can be generalized in many ways.

Computational SVP

Given a basis of L, find $\mathbf{b} \in L$ with $\|\mathbf{b}\| = \lambda_1(L)$.

Decisional SVP

Given a basis of L and a rational d, reply YES is $\lambda_1(L) \leq d$ and NO otherwise.

- We are mostly interested in SVP when the lattice dimension grows to infinity.
- [Van Emde Boas'81]: DecSVP is NP-hard for the infinity norm.
- [Ajtai'98]: DecSVP is NP-hard under randomized reductions.

The Shortest Vector Problem

It comes in many flavours, and can be generalized in many ways.

Computational SVP

Given a basis of L, find $\mathbf{b} \in L$ with $\|\mathbf{b}\| = \lambda_1(L)$.

Decisional SVP

Given a basis of L and a rational d, reply YES is $\lambda_1(L) \leq d$ and NO otherwise.

- We are mostly interested in SVP when the lattice dimension grows to infinity.
- [Van Emde Boas'81]: DecSVP is NP-hard for the infinity norm.
- [Ajtai'98]: DecSVP is NP-hard under randomized reductions.

Variants of SVP

SVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda_1(L)$.

GapSVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L and a rational d, reply YES if $\lambda_1(L) \leq d$ and NO if $\lambda_1(L) \geq \gamma \cdot d$.

- [HavReg'07]: GapSVP_γ is NP-hard for any $\gamma \leq 2^{(\log n)^{1-\varepsilon}}$, under randomized reductions.
- [AhaReg'04]: GapSVP_γ is in NP $\cap$ coNP when $\gamma \geq \sqrt{n}$.
  $\Rightarrow$ GapSVP_γ is unlikely to be NP-hard for such γ.
- Best polynomial-time algorithm achieves $\gamma = 2^{O\left(\frac{n \log \log n}{\log n}\right)}$.

Variants of SVP

SVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda_1(L)$.

GapSVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L and a rational d, reply YES if $\lambda_1(L) \leq d$ and NO if $\lambda_1(L) \geq \gamma \cdot d$.

- [HavReg'07]: GapSVP_γ is NP-hard for any $\gamma \leq 2^{(\log n)^{1-\varepsilon}}$, under randomized reductions.
- [AhaReg'04]: GapSVP_γ is in NP $\cap$ coNP when $\gamma \geq \sqrt{n}$.
$\Rightarrow$ GapSVP_γ is unlikely to be NP-hard for such γ.
- Best polynomial-time algorithm achieves $\gamma = 2^{O\left(\frac{n \log\log n}{\log n}\right)}$.

Variants of SVP

SVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda_1(L)$.

GapSVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L and a rational d, reply YES if $\lambda_1(L) \leq d$ and NO if $\lambda_1(L) \geq \gamma \cdot d$.

- [HavReg'07]: GapSVP_γ is NP-hard for any $\gamma \leq 2^{(\log n)^{1-\varepsilon}}$, under randomized reductions.
- [AhaReg'04]: GapSVP_γ is in NP $\cap$ coNP when $\gamma \geq \sqrt{n}$.
  $\Rightarrow$ GapSVP_γ is unlikely to be NP-hard for such γ.
- Best polynomial-time algorithm achieves $\gamma = 2^{O\left(\frac{n \log\log n}{\log n}\right)}$.

Variants of SVP

SVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda_1(L)$.

GapSVP_γ for approximation factor $\gamma \geq 1$

Given a basis of L and a rational d, reply YES if $\lambda_1(L) \leq d$ and NO if $\lambda_1(L) \geq \gamma \cdot d$.

- [HavReg'07]: GapSVP_γ is NP-hard for any $\gamma \leq 2^{(\log n)^{1-\varepsilon}}$, under randomized reductions.
- [AhaReg'04]: GapSVP_γ is in NP $\cap$ coNP when $\gamma \geq \sqrt{n}$.
  $\Rightarrow$ GapSVP_γ is unlikely to be NP-hard for such γ.
- Best polynomial-time algorithm achieves $\gamma = 2^{O\left(\frac{n \log \log n}{\log n}\right)}$.

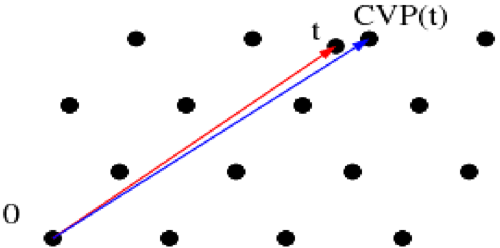
The Closest Vector Problem

CVP_γ for $\gamma \geq 1$

Given a basis of L and a vector $\mathbf{t}$, find $\mathbf{b} \in L$ s.t. $0 < \|\mathbf{b} - \mathbf{t}\| \leq \gamma \cdot \mathrm{dist}(\mathbf{t}, L)$.

GapCVP_γ for $\gamma \geq 1$

Given a basis of L, a vector $\mathbf{t}$ and a rational d, reply YES if $\mathrm{dist}(\mathbf{t}, L) \leq d$ and NO if $\mathrm{dist}(\mathbf{t}, L) \geq \gamma \cdot d$.



Plenty of variants (1/2)

uSVP$_\gamma$ (Unique SVP)

Given a basis of L s.t. $\lambda_2(L) \geq \gamma \cdot \lambda_1(L)$, find $\mathbf{b} \in L$ such that $\|\mathbf{b}\| = \lambda_1(L)$.

HSVP$_\gamma$ (Hermite SVP)

Given a basis of L, find $\mathbf{b} \in L$ such that $\|\mathbf{b}\| \leq \gamma \cdot (\det L)^{1/n}$.

BDD$_\gamma$ (Bounded Distance Decoding)

Given a basis of L and a vector $\mathbf{t}$ such that $\mathrm{dist}(\mathbf{t}, L) \leq \frac{1}{\gamma}\lambda_1(L)$, find $\mathbf{b} \in L$ that is closest to $\mathbf{t}$.

Plenty of variants (1/2)

uSVP_γ (Unique SVP)

Given a basis of L s.t. $\lambda_2(L) \geq \gamma \cdot \lambda_1(L)$, find $\mathbf{b} \in L$ such that $\|\mathbf{b}\| = \lambda_1(L)$.

HSVP_γ (Hermite SVP)

Given a basis of L, find $\mathbf{b} \in L$ such that $\|\mathbf{b}\| \leq \gamma \cdot (\det L)^{1/n}$.

BDD_γ (Bounded Distance Decoding)

Given a basis of L and a vector $\mathbf{t}$ such that $\mathrm{dist}(\mathbf{t}, L) \leq \frac{1}{\gamma}\lambda_1(L)$, find $\mathbf{b} \in L$ that is closest to $\mathbf{t}$.

Plenty of variants (2/2)

SIVP_γ (Shortest Independent Vectors Problem)

Given a basis of L of dimension n, find $\mathbf{b}_1, \ldots, \mathbf{b}_n \in L$ linearly independent such that $\max_i \|\mathbf{b}_i\| \leq \gamma \cdot \lambda_n(L)$.

SBP_γ (Shortest Basis Problem)

Given a basis of L, find a basis $(\mathbf{b}_i)_i$ of L such that $\max \|\mathbf{b}_i\| \leq \gamma \cdot \min_{(\mathbf{c}_i)_i \text{ basis}} \max \|\mathbf{c}_i\|$.

Much more on this topic in “Complexity of lattice problems” by Micciancio and Goldwasser (2002).
See also [Mic'08,LyuMic'09].

Plenty of variants (2/2)

SIVP_γ (Shortest Independent Vectors Problem)

Given a basis of L of dimension n, find $\mathbf{b}_1, \ldots, \mathbf{b}_n \in L$ linearly independent such that $\max_i \|\mathbf{b}_i\| \leq \gamma \cdot \lambda_n(L)$.

SBP_γ (Shortest Basis Problem)

Given a basis of L, find a basis $(\mathbf{b}_i)_i$ of L such that $\max \|\mathbf{b}_i\| \leq \gamma \cdot \min_{(\mathbf{c}_i)_i \text{ basis}} \max \|\mathbf{c}_i\|$.

Much more on this topic in "Complexity of lattice problems" by Micciancio and Goldwasser (2002).
See also [Mic'08,LyuMic'09].

General rules to be remembered about all these problems

- Easier when γ increases.
- Often somewhat NP-hard for very small γ.
- Typically not NP hard for polynomial γ
(the kind of γ used in cryptography).
- Solvable in polynomial-time for γ almost exponential in n

The lattice algorithms rule of thumb

Given a basis of an n-dimensional lattice, the best known algorithms achieve

$$\gamma \approx k^{O(k/n)} \text{ in time } \approx n^{O(1)} \cdot 2^{O(k)}.$$

$\Rightarrow$ Best γ in polynomial-time: $\gamma = 2^{O\left(\frac{n \log\log n}{\log n}\right)}$.

$\Rightarrow$ Complexity $2^{O(n)}$ for polynomial γ.

General rules to be remembered about all these problems

- Easier when γ increases.
- Often somewhat NP-hard for very small γ.
- Typically not NP hard for polynomial γ (the kind of γ used in cryptography).
- Solvable in polynomial-time for γ almost exponential in n

The lattice algorithms rule of thumb

Given a basis of an n-dimensional lattice, the best known algorithms achieve

$$\gamma \approx k^{O(k/n)} \text{ in time } \approx n^{O(1)} \cdot 2^{O(k)}.$$

$\Rightarrow$ Best γ in polynomial-time: $\gamma = 2^{O\left(\frac{n \log \log n}{\log n}\right)}$.

$\Rightarrow$ Complexity $2^{O(n)}$ for polynomial γ.

General rules to be remembered about all these problems

- Easier when γ increases.
- Often somewhat NP-hard for very small γ.
- Typically not NP hard for polynomial γ (the kind of γ used in cryptography).
- Solvable in polynomial-time for γ almost exponential in n

The lattice algorithms rule of thumb

Given a basis of an n-dimensional lattice, the best known algorithms achieve

$$\gamma \approx k^{O(k/n)} \text{ in time } \approx n^{O(1)} \cdot 2^{O(k)}.$$

$\Rightarrow$ Best γ in polynomial-time: $\gamma = 2^{O\left(\frac{n \log\log n}{\log n}\right)}$.

$\Rightarrow$ Complexity $2^{O(n)}$ for polynomial γ.