Shortest Vector Problem

Marios Georgiou

National Technical University of Athens

May 24, 2011

Contents

Lattice

Lattice

Definition

A *Lattice* $\mathcal{L}$ in $\Re^n$ is a discrete subgroup of $\Re^n$ which spans the real vector space $\Re^n$.

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{a_i} \mid \lambda_i \in \mathbb{Z} \right\}$$

Lattice

Definition

A *Lattice* $\mathcal{L}$ in $\Re^n$ is a discrete subgroup of $\Re^n$ which spans the real vector space $\Re^n$.

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{a_i} \mid \lambda_i \in \mathbb{Z} \right\}$$

$\mathbf{a_1}, \mathbf{a_2}, \cdots, \mathbf{a_n}$ is a basis of the lattice

Lattice

Definition

A *Lattice* $\mathcal{L}$ in $\Re^n$ is a discrete subgroup of $\Re^n$ which spans the real vector space $\Re^n$.

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{a_i} \mid \lambda_i \in \mathbb{Z} \right\}$$

$\mathbf{a_1}, \mathbf{a_2}, \cdots, \mathbf{a_n}$ is a basis of the lattice

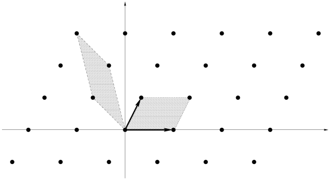


Figure: A Lattice in $\Re^2$

More useful things

More useful things

Theorem

Let $\mathcal{L}$ be a n-dimensional lattice and

- $\mathbf{A}$ *be the $n \times n$ matrix whose rows are the basis* $\mathbf{a_1}, \cdots, \mathbf{a_n}$.
- $\mathbf{B}$ *be the $n \times n$ matrix whose rows* $\mathbf{b_1}, \cdots, \mathbf{b_n} \in \mathcal{L}$.

The following conditions are equivalent:

More useful things

Theorem

Let $\mathcal{L}$ be a n-dimensional lattice and

- $\mathbf{A}$ *be the $n \times n$ matrix whose rows are the basis* $\mathbf{a_1, \cdots, a_n}$.
- $\mathbf{B}$ *be the $n \times n$ matrix whose rows* $\mathbf{b_1, \cdots, b_n} \in \mathcal{L}$.

The following conditions are equivalent:

1. $\mathbf{b_1, \cdots, b_n}$ *form a basis for $\mathcal{L}$.*
2. $|\det(\mathbf{A})| = |\det(\mathbf{B})|$.
3. *there is an $n \times n$ matrix* $\mathbf{U}$ *such that* $\mathbf{B = UA}$ *and* $|\det(\mathbf{U})| = 1$.

More useful things

Theorem

Let $\mathcal{L}$ be a n-dimensional lattice and

- $\mathbf{A}$ *be the $n \times n$ matrix whose rows are the basis* $\mathbf{a_1}, \cdots, \mathbf{a_n}$.
- $\mathbf{B}$ *be the $n \times n$ matrix whose rows* $\mathbf{b_1}, \cdots, \mathbf{b_n} \in \mathcal{L}$.

The following conditions are equivalent:

1. $\mathbf{b_1}, \cdots, \mathbf{b_n}$ *form a basis for* $\mathcal{L}$.
2. $|\det(\mathbf{A})| = |\det(\mathbf{B})|$.
3. *there is an $n \times n$ matrix* $\mathbf{U}$ *such that* $\mathbf{B} = \mathbf{UA}$ *and* $|\det(\mathbf{U})| = 1$.

So the determinant of all the bases of $\mathcal{L}$ is invariable.
$\det(\mathbf{A}) = \det \mathcal{L}$

More useful things

Definition

The *Eucledian norm* of a vector $\mathbf{x}$ is $\|\mathbf{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$ where $x_1, x_2, \cdots, x_n$ are the coefficients in an orthonormal system.

More useful things

Definition

The *Eucledian norm* of a vector $\mathbf{x}$ is $\|\mathbf{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$ where $x_1, x_2, \cdots, x_n$ are the coefficients in an orthonormal system.

Definition

Hadamard's inequality states that $\det \mathcal{L} \leq \|\mathbf{a_1}\| \cdots \|\mathbf{a_n}\|$

More useful things

Definition

The *Eucledian norm* of a vector $\mathbf{x}$ is $\|\mathbf{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}$ where $x_1, x_2, \cdots, x_n$ are the coefficients in an orthonormal system.

Definition

Hadamard's inequality states that $\det \mathcal{L} \leq \|\mathbf{a_1}\| \cdots \|\mathbf{a_n}\|$

Definition

Orthogonality defect of the basis $\mathbf{a_1}, \mathbf{a_2}, \cdots, \mathbf{a_n}$

$$\frac{\|\mathbf{a_1}\| \cdots \|\mathbf{a_n}\|}{\det \mathcal{L}}$$

Primitivity

Definition

The linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_k} \in \mathcal{L}$ are *primitive* if they can be extended to a basis of $\mathcal{L}$.

Primitivity

Definition

The linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_k} \in \mathcal{L}$ are *primitive* if they can be extended to a basis of $\mathcal{L}$.

Definition

A vector $\mathbf{a} \in \mathcal{L}$ is *shortest in its direction* if $x\mathbf{a}$ is not in $\mathcal{L}$ for $0 < x < 1$.

Primitivity

Definition

The linearly independent vectors $\mathbf{b_1}, \cdots, \mathbf{b_k} \in \mathcal{L}$ are *primitive* if they can be extended to a basis of $\mathcal{L}$.

Definition

A vector $\mathbf{a} \in \mathcal{L}$ is *shortest in its direction* if $x\mathbf{a}$ is not in $\mathcal{L}$ for $0 < x < 1$.

Theorem

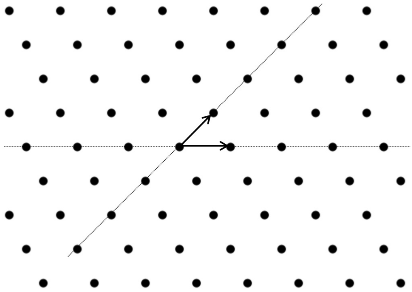
Vector $\mathbf{a} \in \mathcal{L}$ is primitive iff $\mathbf{a}$ is shortest in its direction.

Contents

Shortest vector problem

Definition

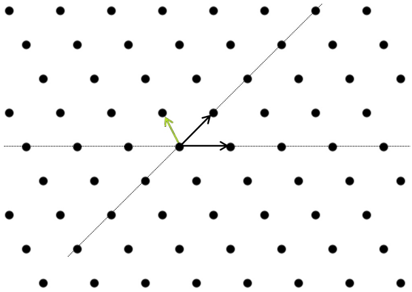
Given a lattice $\mathcal{L}$, find the shortest vector, in Eucledian norm, in $\mathcal{L}$.



Shortest vector problem

Definition

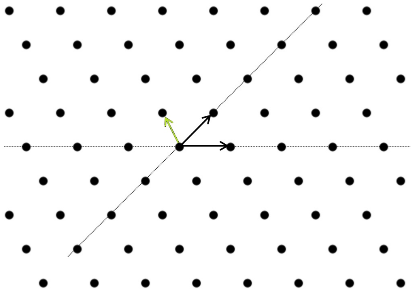
Given a lattice $\mathcal{L}$, find the shortest vector, in Eucledian norm, in $\mathcal{L}$.



Shortest vector problem

Definition

Given a lattice $\mathcal{L}$, find the shortest vector, in Eucledian norm, in $\mathcal{L}$.



The shortest of the basis is not always the shortest vector.

Contents

The main idea

A good strategy:

The main idea

A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).

The main idea

A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).
2. Take the shortest vector of the basis.

The main idea

A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).
2. Take the shortest vector of the basis.

We must prove that this vector is the shortest, or the shortest within some factor.

The main idea

A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).
2. Take the shortest vector of the basis.

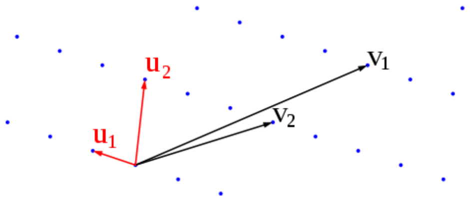
We must prove that this vector is the shortest, or the shortest within some factor.
Step 1 is called *Lattice (Basis) Reduction*

The main idea

A good strategy:

1. Change the basis of the lattice (in some way) to a good one (short vectors nearly orthogonal).
2. Take the shortest vector of the basis.

We must prove that this vector is the shortest, or the shortest within some factor.
Step 1 is called *Lattice (Basis) Reduction*



Algorithm for the 1-dimensional Lattices
Euclid's Algorithm

- Consider an 1-d lattice with basis $a \in \Re$.

Algorithm for the 1-dimensional Lattices
Euclid's Algorithm

- Consider an 1-d lattice with basis $a \in \Re$.
  Then the shortest vector is simply a.

Algorithm for the 1-dimensional Lattices
Euclid's Algorithm

- Consider an 1-d lattice with basis $a \in \Re$.
  Then the shortest vector is simply a.
- Consider an 1-d lattice with basis $a, b \in \Re$.

Algorithm for the 1-dimensional Lattices
Euclid's Algorithm

- Consider an 1-d lattice with basis $a \in \Re$.
  Then the shortest vector is simply a.
- Consider an 1-d lattice with basis $a, b \in \Re$.
  Then the shortest vector is the smallest number expressed as an integer l.c. of a, b:

Algorithm for the 1-dimensional Lattices
Euclid's Algorithm

- Consider an 1-d lattice with basis $a \in \Re$.
  Then the shortest vector is simply a.
- Consider an 1-d lattice with basis $a, b \in \Re$.
  Then the shortest vector is the smallest number expressed as an integer l.c. of a, b: $\gcd(a, b)$.

Algorithm for the 1-dimensional Lattices Euclid's Algorithm

- Consider an 1-d lattice with basis $a \in \Re$.
  Then the shortest vector is simply a.
- Consider an 1-d lattice with basis $a, b \in \Re$.
  Then the shortest vector is the smallest number expressed as an integer l.c. of a, b: $\gcd(a, b)$.
  Euclid's algorithm: $\gcd(a, b) = gcd(b, a - mb)$ where m is the integer closest to a/b.

Algorithm for the 2-dimensional Lattices
Gauss reduced basis

Algorithm for the 2-dimensional Lattices
Gauss reduced basis

How orthogonal our basis vectors have to be?

Algorithm for the 2-dimensional Lattices
Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ *is a basis for a 2-d* $\mathcal{L}$ *and* $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$*. Suppose* $\theta \in (0^\circ, 180^\circ)$ *the angle between the two vectors. If* $60^\circ \leq \theta \leq 120^\circ$ *then* $\mathbf{b_1}$ *is the shortest vector in* $\mathcal{L}$*.*

Algorithm for the 2-dimensional Lattices
Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ *is a basis for a 2-d* $\mathcal{L}$ *and* $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$. *Suppose* $\theta \in (0^\circ, 180^\circ)$ *the angle between the two vectors. If* $60^\circ \leq \theta \leq 120^\circ$ *then* $\mathbf{b_1}$ *is the shortest vector in* $\mathcal{L}$.

Let $\mu_{21}\mathbf{b_1}$ denote the projection of the vector $\mathbf{b_2}$ in the direction of the vector $\mathbf{b_1}$:

Algorithm for the 2-dimensional Lattices
Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ is a basis for a 2-d $\mathcal{L}$ and $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$. Suppose $\theta \in (0^\circ, 180^\circ)$ the angle between the two vectors. If $60^\circ \leq \theta \leq 120^\circ$ then $\mathbf{b_1}$ is the shortest vector in $\mathcal{L}$.

Let $\mu_{21}\mathbf{b_1}$ denote the projection of the vector $\mathbf{b_2}$ in the direction of the vector $\mathbf{b_1}$:

$$\mu_{21} = \frac{\|\mathbf{b_2}\| \cdot \|\mathbf{b_1}\|}{\|\mathbf{b_1}\|^2}$$

Algorithm for the 2-dimensional Lattices
Gauss reduced basis

How orthogonal our basis vectors have to be?

Theorem

Suppose $\mathbf{b_1}, \mathbf{b_2}$ is a basis for a 2-d $\mathcal{L}$ and $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$. Suppose $\theta \in (0^\circ, 180^\circ)$ the angle between the two vectors. If $60^\circ \leq \theta \leq 120^\circ$ then $\mathbf{b_1}$ is the shortest vector in $\mathcal{L}$.

Let $\mu_{21}\mathbf{b_1}$ denote the projection of the vector $\mathbf{b_2}$ in the direction of the vector $\mathbf{b_1}$:

$$\mu_{21} = \frac{\|\mathbf{b_2}\| \cdot \|\mathbf{b_1}\|}{\|\mathbf{b_1}\|^2}$$

If $\|\mathbf{b_1}\| \leq \|\mathbf{b_2}\|$ and $|\mu_{21}| \leq 1/2$ then the basis $\mathbf{b_1}, \mathbf{b_2}$ is Gauss reduced basis.

Gauss's Algorithm

Algorithm for S.V. in 2-d

repeat
  if $\|\mathbf{b_1}\| > \|\mathbf{b_2}\|$ **then**
    swap $\mathbf{b_1}, \mathbf{b_2}$
  end if
  $m \leftarrow \lfloor \mu_{21} \rceil$
  $\mathbf{b_2} \leftarrow \mathbf{b_2} - m\mathbf{b_1}$
until $\|\mathbf{b_1}\| < \|\mathbf{b_2}\|$
return $\mathbf{b_1}$

Gauss's Algorithm

Algorithm for S.V. in 2-d

repeat
  if $\|\mathbf{b_1}\| > \|\mathbf{b_2}\|$ **then**
    swap $\mathbf{b_1}, \mathbf{b_2}$
  end if
  $m \leftarrow \lfloor \mu_{21} \rceil$
  $\mathbf{b_2} \leftarrow \mathbf{b_2} - m\mathbf{b_1}$
until $\|\mathbf{b_1}\| < \|\mathbf{b_2}\|$
return $\mathbf{b_1}$

- Similarity with the Euclidean Algorithm

Gauss's Algorithm

Algorithm for S.V. in 2-d

repeat
  if $\|\mathbf{b_1}\| > \|\mathbf{b_2}\|$ **then**
    swap $\mathbf{b_1}, \mathbf{b_2}$
  end if
  $m \leftarrow \lfloor \mu_{21} \rceil$
  $\mathbf{b_2} \leftarrow \mathbf{b_2} - m\mathbf{b_1}$
until $\|\mathbf{b_1}\| < \|\mathbf{b_2}\|$
return $\mathbf{b_1}$

- Similarity with the Euclidean Algorithm
- Terminates in a finite amount of time

Gauss's Algorithm

Algorithm for S.V. in 2-d

repeat
  if $\|\mathbf{b_1}\| > \|\mathbf{b_2}\|$ **then**
    swap $\mathbf{b_1}, \mathbf{b_2}$
  end if
  $m \leftarrow \lfloor \mu_{21} \rceil$
  $\mathbf{b_2} \leftarrow \mathbf{b_2} - m\mathbf{b_1}$
until $\|\mathbf{b_1}\| < \|\mathbf{b_2}\|$
return $\mathbf{b_1}$

- Similarity with the Euclidean Algorithm
- Terminates in a finite amount of time
- Polynomial complexity

Contents

Gram-Schmidt orthogonalization

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ the basis of $\mathcal{L}$.

Gram-Schmidt orthogonalization

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ the basis of $\mathcal{L}$. The *Gram-Schmidt orthogonalization* of this basis is: $\mathbf{b_1^*} \cdots \mathbf{b_n^*}$ and is given by the following iterative formula:

$$\mathbf{b_1^*} = \mathbf{b_1}$$

$$\mathbf{b_i^*} = \mathbf{b_i} - \sum_{j=1}^{i-1} \frac{\mathbf{b_i b_j^*}}{\|\mathbf{b_j^*}\|^2} \mathbf{b_j^*}$$

Gram-Schmidt orthogonalization

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ the basis of $\mathcal{L}$. The *Gram-Schmidt orthogonalization* of this basis is: $\mathbf{b_1^*} \cdots \mathbf{b_n^*}$ and is given by the following iterative formula:

$$\mathbf{b_1^*} = \mathbf{b_1}$$

$$\mathbf{b_i^*} = \mathbf{b_i} - \sum_{j=1}^{i-1} \frac{\mathbf{b_i b_j^*}}{\|\mathbf{b_j^*}\|^2} \mathbf{b_j^*}$$

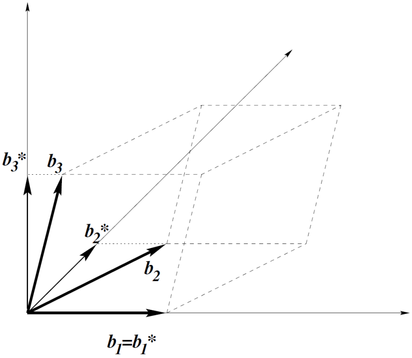
Define

$$\mu_{ij} = \frac{\mathbf{b_i b_j^*}}{\|\mathbf{b_j^*}\|^2}$$

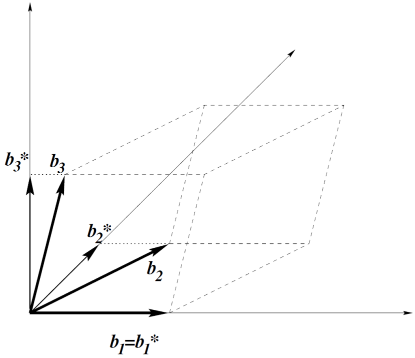
and $\mu_{ii} = 1$. Then

$$\mathbf{b_i} = \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b_j^*}$$

Lower bounding OPT



Lower bounding OPT



If OPT is the length of the shortest vector in the lattice then:

$$OPT \geq min\{\|\mathbf{b_1^*}\|, \cdots, \|\mathbf{b_n^*}\|\}$$

LLL Reduced Basis

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \leq i \leq n-1$:

LLL Reduced Basis

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \leq i \leq n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b_i^*}\|^2 \leq \frac{4}{3}\|\mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}\|^2$

LLL Reduced Basis

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \leq i \leq n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b_i^*}\|^2 \leq \frac{4}{3}\|\mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}\|^2$

An LLL Reduced Basis is reasonably orthogonal:

$$\frac{\|\mathbf{b_1}\| \cdots \|\mathbf{b_n}\|}{\det \mathcal{L}} \leq 2^{\frac{n(n-1)}{2}}$$

LLL Reduced Basis

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \leq i \leq n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b_i^*}\|^2 \leq \frac{4}{3}\|\mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}\|^2$

An LLL Reduced Basis is reasonably orthogonal:

$$\frac{\|\mathbf{b_1}\| \cdots \|\mathbf{b_n}\|}{\det \mathcal{L}} \leq 2^{\frac{n(n-1)}{2}}$$

In an LLL Reduced Basis we have that:

$$\|\mathbf{b_1}\| \leq 2^{\frac{n-1}{2}} OPT$$

LLL Reduced Basis

The basis $\mathbf{b_1}, \cdots, \mathbf{b_n}$ is LLL reduced if for $1 \leq i \leq n-1$:

- $|\mu_{ij}| \leq \frac{1}{2}$ for $1 \leq i < j \leq n$ and
- $\|\mathbf{b_i^*}\|^2 \leq \frac{4}{3}\|\mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}\|^2$

An LLL Reduced Basis is reasonably orthogonal:

$$\frac{\|\mathbf{b_1}\| \cdots \|\mathbf{b_n}\|}{\det \mathcal{L}} \leq 2^{\frac{n(n-1)}{2}}$$

In an LLL Reduced Basis we have that:

$$\|\mathbf{b_1}\| \leq 2^{\frac{n-1}{2}} OPT$$

So we want an algorithm which turns an arbitrary basis into an LLL reduced in polynomial time in n.

Contents

Shortest vector Algorithm

LLL $(\mathbf{B} = \mathbf{b_1}, \cdots, \mathbf{b_n})$

  $\mathbf{B} \leftarrow \mathit{SizeReduce}(\mathbf{B})$

  while $\exists i$ violating $\|\mathbf{b_i^*}\|^2 \leq \frac{4}{3}\|\mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}\|^2$ **do**

    swap $\mathbf{b_i}, \mathbf{b_{i+1}}$

    update μ_{hk} and $\mathbf{b_k^*}$ for all h, k

    $\mathbf{B} \leftarrow \mathit{SizeReduce}(\mathbf{B})$

  end while

  return $\mathbf{b_1}$

SizeReduce $(\mathbf{B} = \mathbf{b_1}, \cdots, \mathbf{b_n})$

  for $j = 2, \cdots, n$ **do**

    for $i = j - 1, \cdots, 1$ **do**

      $\mathbf{b_j} \leftarrow \mathbf{b_j} - \lfloor \mu_{ji}\mathbf{b_i} \rceil$

      $\mu_{jk} \leftarrow \mu_{jk} - \mu_{ji}\mathbf{b_i}\mu_{ik}$ for $k = 1, \cdots, i$

    end for

  end for

  return $\mathbf{B}$

Contents

The dual lattice $\mathcal{L}^*$

The dual lattice $\mathcal{L}^*$

Definition

The *dual lattice* $\mathcal{L}^*$ of the lattice $\mathcal{L}$ is defined by:

$$\mathcal{L}^* = \{\boldsymbol{v} \in \Re^n | \forall \mathbf{b} \in \mathcal{L}, \mathbf{b} \cdot \boldsymbol{v} \in \mathbb{Z}\}$$

The dual lattice $\mathcal{L}^*$

Definition

The *dual lattice* $\mathcal{L}^*$ of the lattice $\mathcal{L}$ is defined by:

$$\mathcal{L}^* = \{\boldsymbol{v} \in \Re^n | \forall \mathbf{b} \in \mathcal{L}, \mathbf{b} \cdot \boldsymbol{v} \in \mathbb{Z}\}$$

Theorem

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ be any basis for $\mathcal{L}$. Then, the rows of $\mathbf{B^{-T}}$ form a basis for the dual lattice $\mathcal{L}^*$. Furthermore, $\det \mathcal{L}^* = \frac{1}{\det \mathcal{L}}$.

The dual lattice $\mathcal{L}^*$

Definition

The *dual lattice* $\mathcal{L}^*$ of the lattice $\mathcal{L}$ is defined by:

$$\mathcal{L}^* = \{\boldsymbol{v} \in \Re^n | \forall \mathbf{b} \in \mathcal{L}, \mathbf{b} \cdot \boldsymbol{v} \in \mathbb{Z}\}$$

Theorem

Let $\mathbf{b_1} \cdots \mathbf{b_n}$ *be any basis for* $\mathcal{L}$*. Then, the rows of* $\mathbf{B}^{-\mathbf{T}}$ *form a basis for the dual lattice* $\mathcal{L}^*$*. Furthermore,* $\det \mathcal{L}^* = \frac{1}{\det \mathcal{L}}$.

Definition

Let $\boldsymbol{v} \in \Re^n$ be a non-zero vector. Then, $\boldsymbol{v}^\perp$ will denote the $(n-1)$-dimensional space $\{\mathbf{b} \in \Re^n | \mathbf{b} \cdot \boldsymbol{v} = 0\}$

The dual lattice $\mathcal{L}^*$

Definition

A set $\mathcal{L}' \subset \mathcal{L}$ that is a lattice in its own right will be called *sublattice* of $\mathcal{L}$

The dual lattice $\mathcal{L}^*$

Definition

A set $\mathcal{L}' \subset \mathcal{L}$ that is a lattice in its own right will be called *sublattice* of $\mathcal{L}$

Lemma

Let $\boldsymbol{v} \in \mathcal{L}^*$ be primitive. Then

- $\mathcal{L} \cap (\boldsymbol{v}^\perp)$ *is an* $(n-1)$*-dimensional sublattice of* $\mathcal{L}$.
- *There is a vector* $\mathbf{b} \in \mathcal{L}$ *such that* $\boldsymbol{v} \cdot \mathbf{b} = 1$

The dual lattice $\mathcal{L}^*$

Definition

A set $\mathcal{L}' \subset \mathcal{L}$ that is a lattice in its own right will be called *sublattice* of $\mathcal{L}$

Lemma

Let $\boldsymbol{v} \in \mathcal{L}^*$ be primitive. Then

- $\mathcal{L} \cap (\boldsymbol{v}^{\perp})$ *is an* $(n-1)$*-dimensional sublattice of* $\mathcal{L}$.
- *There is a vector* $\mathbf{b} \in \mathcal{L}$ *such that* $\boldsymbol{v} \cdot \mathbf{b} = 1$

Lemma

We can create a basis $\mathbf{w}_n, \cdots, \mathbf{w}_1$ *with Gram-Schmidt orthogonalization* $\left(\frac{\boldsymbol{v}_n}{\|\boldsymbol{v}_n\|^2}, \cdots, \frac{\boldsymbol{v}_1}{\|\boldsymbol{v}_1\|^2}\right)$.

Contents

Gram-Schmidt lower bound is not so bad

Gram-Schmidt lower bound is not so bad

Minkowski's theorem

There is a vector $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{b}\| \leq \sqrt{n}\sqrt[n]{\det \mathcal{L}}$.

Gram-Schmidt lower bound is not so bad

Minkowski's theorem

There is a vector $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{b}\| \leq \sqrt{n}\sqrt[n]{\det \mathcal{L}}$.

Theorem

There is a basis for $\mathcal{L}$ whose Gram-Schmidt lower bound is at least OPT/n.

Contents

Solving modular equations

Solving modular equations

Lemma

If f is a polynomial modulo n and h is a polynomial having the same roots as f modulo n and has 'small' norm then all the roots of f (smaller than some value) are also roots of h over the integers.

Solving modular equations

Lemma

If f is a polynomial modulo n and h is a polynomial having the same roots as f modulo n and has 'small' norm then all the roots of f (smaller than some value) are also roots of h over the integers.

The LLL algorithm can find such a polynomial h and then solve the equation $h(x) = 0$ over the integers to get small solutions.

QUESTIONS