Lattices and LLL algorithm

for MS Seminar

Kushagra Shandilya - 21Q050010
kushagras@cse.iitb.ac.in

Indian Institute of Technology, Bombay

13 April, 2022

Contents

Cauchy-Schwarz inequality

$|\langle a, b\rangle|^2 \leq \langle a, a\rangle \cdot \langle b, b\rangle$ or

$|\langle a, b\rangle| \leq ||a|| \cdot ||b||$

Lattice

Definition

(Lattice) Given n linearly independent vectors $b_1, b_2, \dots b_n \in \mathbb{R}^m$, the lattice generated by them is defined as

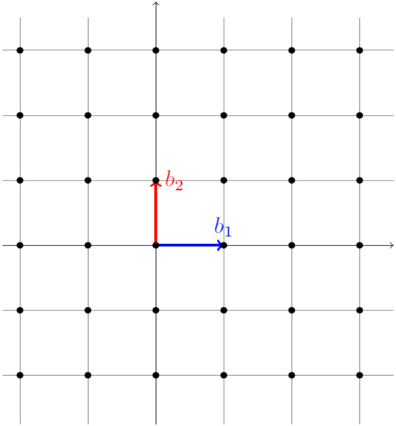
$$\mathcal{L}(b_1, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \;\middle|\; x_i \in \mathbb{Z} \right\}$$

In matrix form, $\mathcal{L}(\mathbf{B}) = \{\mathbf{B}x \mid x \in \mathbb{Z}^n\}$

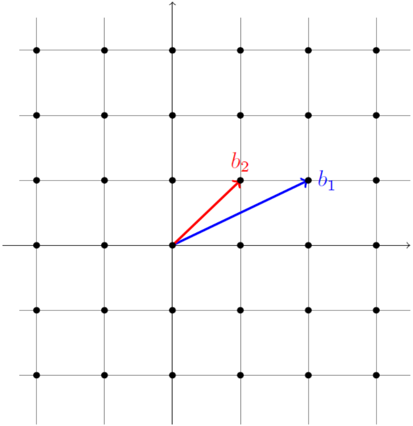
Definition

(Lattice) A lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$.

Examples of Lattices I

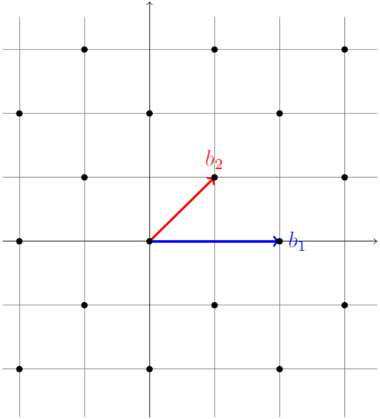


(A) The lattice $\mathbb{Z}^2$ with basis vectors $(0, 1)$ and $(1, 0)$.

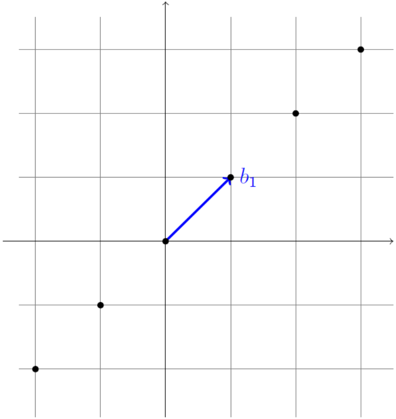


(B) The lattice $\mathbb{Z}^2$ with a different basis consisting of vectors $(2, 1)$ and $(1, 1)$.

Examples of Lattices II



(C) A full-rank lattice generated by the basis vectors $(2,0)$ and $(1,1)$. This is a sub-lattice of $\mathbb{Z}^2$.



(D) A *non full-rank* lattice with basis vector $(1,1)$

Algebraic Characterization using Unimodular Matrices I

Definition

(Unimodular matrix) A matrix $\boldsymbol{U} \in \mathbb{Z}^{n \times n}$ is Unimodular if $|det(\boldsymbol{U})| = 1$ where $|.|$ represents the absolute value.

Lemma

If $\boldsymbol{U}$ is Unimodular, so is $\boldsymbol{U}^{-1}$.

Proof.

- $\boldsymbol{U}^{-1} = adj(\boldsymbol{U})/det(\boldsymbol{U})$
- $|det(\boldsymbol{U}^{-1})| = 1/|det(\boldsymbol{U})| = 1$

□

Algebraic Characterization using Unimodular Matrices II

Theorem

Given two full rank bases $B, B' \in \mathbb{R}^{n \times n}$, $\mathcal{L}(B) = \mathcal{L}(B')$ *if and only if there exists an Unimodular matrix* U *such that* $B' = BU$.

Proof.

($\Rightarrow$) Suppose $\mathcal{L}(B) = \mathcal{L}(B')$.
For each b_i column of B', $b' \in \mathcal{L}(B)$. Thus, $B' = BU$. Similarly, $B = B'V$.
$B = B'V = BUV \quad \Rightarrow \quad UV = I_n \quad \Rightarrow \quad det(U)det(V) = 1$
U and V are integer matrices. Thus, $|det(U)| = |det(V)| = 1$.

($\Leftarrow$) Suppose $\exists$ an Unimodular matrix U such that $B' = BU$.
For each b_i column of B', $b_i \in \mathcal{L}(B)$. Thus, $\mathcal{L}(B') \subseteq \mathcal{L}(B)$.
Similarly, $B = B'U^{-1}$, thus, $\mathcal{L}(B) \subseteq \mathcal{L}(B')$. Therefore, $\mathcal{L}(B) = \mathcal{L}(B')$. $\square$

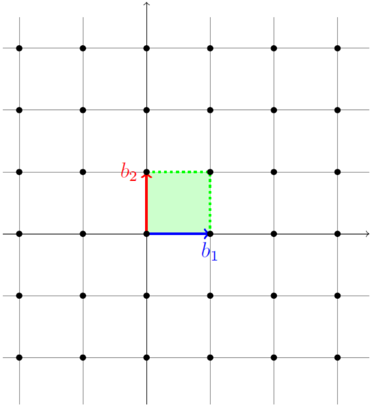
Fundamental Parallelepiped

Definition

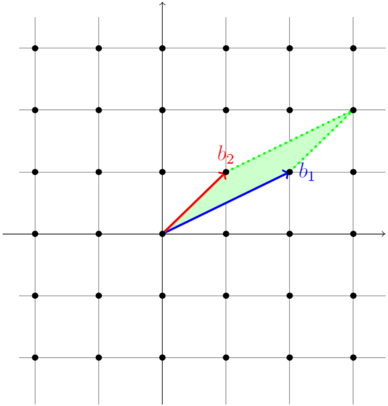
(Fundamental Parallelepiped) Given n linearly independent vectors $b_1, b_2, ...b_n \in \mathbb{R}^m$, their fundamental parallelepiped is defined as

$$\mathcal{P}(b_1, ..., b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid 0 \leq x_i < 1 \right\}$$

Examples of Fundamental Parallelepiped I

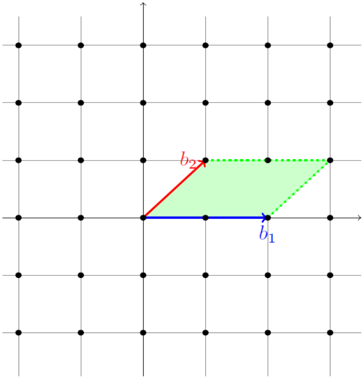


(A) The lattice $\mathbb{Z}^2$ with basis vectors $(0,1)$ and $(1,0)$ and the associated fundamental parallelepiped.



(B) The lattice $\mathbb{Z}^2$ with a different basis consisting of vectors $(2,1)$ and $(1,1)$, and the associated fundamental parallelepiped.

Examples of Fundamental Parallelepiped II



(A) Basis vectors $(2,0)$ and $(1,1)$ do not form the lattice $\mathbb{Z}^2$.

Geometric Characterization using Fundamental Parallelepiped I

Theorem

Let Λ be a full rank n-dimensional lattice, and let $b_1, ..., b_n \in \Lambda$ be n linearly independent vectors. Then, $b_1, ..., b_n$ forms a basis of Λ if and only if $\mathcal{P}(b_1, ..., b_n) \cap \Lambda = \{0\}$.

Equivalent lattices

Lemma

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

- $b_i \leftarrow b_i + kb_j$ *for some* $k \in \mathbb{Z}$
- $b_i \leftrightarrow b_j$
- $b_i \leftarrow -b_i$

$$\begin{bmatrix} 7 & 8 & 2 \\ 3 & 4 & 1 \\ 1 & 3 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 7 & 2 \\ 4 & 3 & 1 \\ 3 & 1 & 1 \end{bmatrix}$$

$b_1 \leftrightarrow b_2$

$$\begin{bmatrix} 7 & 8 & 2 \\ 3 & 4 & 1 \\ 1 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 22 & 2 \\ 3 & 10 & 1 \\ 1 & 5 & 1 \end{bmatrix}$$

$b_2 \leftarrow b_2 + 2b_1$

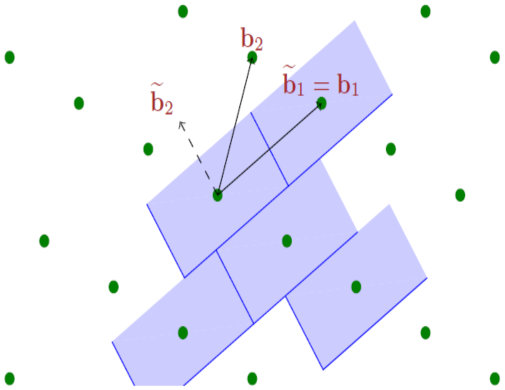
Determinant of a lattice

Definition

The determinant of a lattice $\mathcal{L}(B)$ is defined as the volume of the fundamental parallelepiped formed by its basis vectors.

- Fundamental parallepipeds corresponding to different basis of the same lattice produces the same volume.
  $B' = BU$
  Determinant is a lattice invariant.
- Greater the determinant, sparser the lattice

Gram-Schmidt Orthogonalization I



Gram-Schmidt Orthogonalization II

Definition

For a sequence of n linearly independent vectors $b_1, \ldots, b_n \in \mathbb{R}^m$, Gram-Schmidt Orthogonalization is the procedure to convert $b_1, \ldots, b_n$ into a sequence of orthogonal vectors $\tilde{b}_1, \ldots, \tilde{b}_n$. It is computed as the following

$$\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}_j \qquad \text{where } \mu_{i,j} = \frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle}$$

- A Gram-Schmidt vector $\tilde{b}_i$ is the component of b_i which is orthogonal to the span of $(\tilde{b}_1, \tilde{b}_2, \ldots, \tilde{b_{i-1}})$.
- The first Gram-Schmidt vector $\tilde{b}_1$ is b_1 itself.
- Span of $(\tilde{b}_1, \ldots, \tilde{b}_i)$ is the same as of $(b_1, \ldots, b_i)$ $\quad 1 \leq i \leq n$
- Gram-Schmidt vectors do not necessarily form a lattice basis. They might not even be part of the lattice.
- Gram-Schmidt vectors depend on the order in which basis vectors are sequenced.

Gram-Schmidt Orthogonalization III

$\tilde{b_1} = b_1$
$\tilde{b_2} = b_2 - \mu_{2,1}\tilde{b_1}$
$\tilde{b_3} = b_3 - \mu_{3,1}\tilde{b_1} - \mu_{3,2}\tilde{b_2}$ and so on

$$\begin{pmatrix} | & & | \\ b_1 & \dots & b_n \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ \tilde{b_1} & \dots & \tilde{b_n} \\ | & & | \end{pmatrix} \cdot \begin{pmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \dots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & \dots & \mu_{n,2} \\ 0 & 0 & 1 & \dots & \mu_{n,3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} | & & | \\ \frac{\tilde{b_1}}{||\tilde{b_1}||} & \dots & \frac{\tilde{b_n}}{||\tilde{b_n}||} \\ | & & | \end{pmatrix} \cdot \begin{pmatrix} ||\tilde{b_1}|| & \mu_{2,1}||\tilde{b_1}|| & \mu_{3,1}||\tilde{b_1}|| & \dots & \mu_{n,1}||\tilde{b_1}|| \\ 0 & ||\tilde{b_2}|| & \mu_{3,2}||\tilde{b_2}|| & \dots & \mu_{n,2}||\tilde{b_2}|| \\ 0 & 0 & ||\tilde{b_3}|| & \dots & \mu_{n,3}||\tilde{b_3}|| \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & ||\tilde{b_n}|| \end{pmatrix}$$

Gram-Schmidt Orthogonalization IV

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

First Minima I

Definition

Length of the shortest non-zero vector in the lattice. Denoted by $\lambda_1(\mathcal{L})$.

Theorem

Let B be a rank-n lattice basis and $\tilde{B}$ be its Gram-Schmidt orthogonalization. Then,

$$\lambda_1(\mathcal{L}(B)) \geq \min_{i=1,..,n} ||\tilde{b}_i||$$

Proof.

Let $j \in 1, ..., n$ be the largest index such that $x_j \neq 0$. Then,

$$|\langle Bx, \tilde{b}_j \rangle| = \left| \langle \textstyle\sum_{i=1}^n x_i b_i, \tilde{b}_j \rangle \right| = \left| \textstyle\sum_{i=1}^n \langle x_i b_i, \tilde{b}_j \rangle \right| = |x_j \langle b_j, \tilde{b}_j \rangle| = |x_j \langle \tilde{b}_j, \tilde{b}_j \rangle| = |x_j| \cdot ||\tilde{b}_j||^2$$

First Minima II

$$|\langle Bx, \tilde{b}_j \rangle| \leq ||Bx|| \cdot ||\tilde{b}_j||$$

Together,

$$||Bx|| \geq |x_j| \cdot ||\tilde{b}_j|| \geq ||\tilde{b}_j|| \geq \min_{i=1,..,n} ||\tilde{b}_i||$$

Thus,

$$\lambda_1(\mathcal{L}) \geq \min_{i=1,..,n} ||\tilde{b}_i||$$

$\square$

Lattice Computational Problems

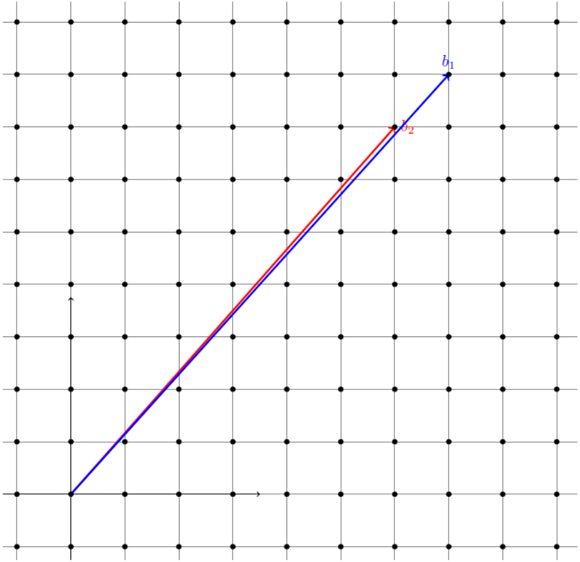
Definition

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

Definition

(Search SVP$_\gamma$) Given a lattice basis $B \in \mathbb{Z}^{m \times n}$, find a non-zero lattice vector v such that $||v|| \leq \gamma \cdot \lambda_1(\mathcal{L}(B))$.

LLL I



(a) The lattice $\mathbb{Z}^2$ with basis vectors $(7, 8)$ and $(6, 7)$.

LLL II

- Polynomial time approximation algorithm
- Approximation factor exponential in n
- Outputs "nearly-orthogonalized" "short" vectors
- In GS orthogonalization $\tilde{b_i} = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b_j}$ *where* $\mu_{i,j} = \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle}$
- In LLL $b_i \leftarrow b_i - c_{i,j} \cdot b_j$ where $c_{i,j} = \lceil \mu_{i,j} \rfloor$

δ-LLL-reduced basis

Definition

(δ-LLL-reduced basis) A basis $B \in \mathbb{R}^{n \times n}$ is δ-LLL reduced if it satisfies the following properties

- $|\mu_{i,j}| \leq \frac{1}{2} \quad \forall\, 1 \leq i \leq n, j < i$
- $\delta ||\tilde{b}_i||^2 \leq ||\mu_{i+1,i} \cdot \tilde{b}_i + \tilde{b}_{i+1}||^2 \quad \forall\, 1 \leq i < n$

Second property

$$\delta||\tilde{b}_i||^2 \leq ||\mu_{i+1,i} \cdot \tilde{b}_i + \tilde{b}_{i+1}||^2 = \mu_{i+1,i}^2||\tilde{b}_i||^2 + ||\tilde{b}_{i+1}||^2$$
$$||\tilde{b}_{i+1}||^2 \geq (\delta - \mu_{i+1,i}^2)||\tilde{b}_i||^2$$
$$||\tilde{b}_{i+1}||^2 \geq \left(\delta - \frac{1}{4}\right)||\tilde{b}_i||^2$$

LLL works when $\frac{1}{4} < \delta < 1$.

First property

$$\begin{pmatrix} ||\tilde{b_1}|| & \leq \frac{1}{2}||\tilde{b_1}|| & \leq \frac{1}{2}||\tilde{b_1}|| & \dots & \leq \frac{1}{2}||\tilde{b_1}|| \\ 0 & ||\tilde{b_2}|| & \leq \frac{1}{2}||\tilde{b_2}|| & \dots & \leq \frac{1}{2}||\tilde{b_2}|| \\ 0 & 0 & ||\tilde{b_3}|| & \dots & \leq \frac{1}{2}||\tilde{b_3}|| \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & ||\tilde{b_n}|| \end{pmatrix}$$

Search SVP$_\gamma$ I

Lemma

Let $b_1, ..., b_n \in \mathbb{R}^n$ be a reduced basis. Then

$$||b_1|| \leq \left(\delta - \frac{1}{4}\right)^{-(n-1)/2} \cdot \lambda_1(\mathcal{L})$$

Proof.

$$||\tilde{b_n}||^2 \geq \left(\delta - \tfrac{1}{4}\right)||\tilde{b}_{n-1}||^2 \geq \cdots \geq \left(\delta - \tfrac{1}{4}\right)^{n-1}||\tilde{b_1}||^2 \geq \left(\delta - \tfrac{1}{4}\right)^{n-1}||b_1||^2$$

$$||b_1|| \leq \left(\delta - \tfrac{1}{4}\right)^{-(i-1)/2}||\tilde{b_i}|| \leq \left(\delta - \tfrac{1}{4}\right)^{-(n-1)/2}||\tilde{b_i}||$$

Search SVP$_\gamma$ II

$$||b_1|| \leq \left(\delta - \frac{1}{4}\right)^{-(n-1)/2} \min_j ||\tilde{b}_j||$$

$$||b_1|| \leq \left(\delta - \frac{1}{4}\right)^{-(n-1)/2} \cdot \lambda_1(\mathcal{L}) \qquad \square$$

LLL algorithm

Given integral basis vectors $b_1, ..., b_n$ as input, do the following:

1 Compute $\tilde{b_1}, ..., \tilde{b_n}$ using Gram-Schmidt Orthogonalization

2 Reduction step:

for $i = 2$ *to* n **do**

    for $j = i - 1$ *to* 1 **do**

$$b_i \leftarrow b_i - c_{i,j} \cdot b_j \text{ where } c_{i,j} = \left\lceil \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} \right\rfloor$$

    end

end

3 Swap step:

if *for any* $i, \delta||\tilde{b_i}||^2 > ||\mu_{i+1,i} \cdot \tilde{b_i} + \tilde{b}_{i+1}||^2$ **then**

    swap b_i with b_{i+1}

    goto step 1

end

4 Output $b_1, ..., b_n$

Observations

- Swap step enforces the second property
- Lattice remains the same during the reduction step
- Gram-Schmidt vectors remains the same during the reduction step

Since we restrict the operation $b_i \leftarrow b_i + ab_j$ for $i > j$

$$B = \begin{bmatrix} b_1 & b_2 & b_3 \end{bmatrix} \qquad \tilde{B} = \begin{bmatrix} \tilde{b_1} & \tilde{b_2} & \tilde{b_3} \end{bmatrix}$$

$$B' = \begin{bmatrix} b_1 & b_2 & b_3 + kb_2 \end{bmatrix} \qquad \tilde{B}' = \begin{bmatrix} \tilde{b_1} & \tilde{b_2} & \tilde{b_3'} \end{bmatrix}$$

$$B = \tilde{B}U$$

$$BE = \tilde{B}UE$$

$$B' = \tilde{B}U'$$

$$\begin{aligned}
\tilde{b_3'} &= (b_3 + kb_2) - \mu'_{3,1}\tilde{b_1} - \mu'_{3,2}\tilde{b_2} \\
&= (b_3 + kb_2) - \frac{\langle b_3 + kb_2, \tilde{b_1} \rangle}{\langle \tilde{b_1}, \tilde{b_1} \rangle}\tilde{b_1} - \frac{\langle b_3 + kb_2, \tilde{b_2} \rangle}{\langle \tilde{b_2}, \tilde{b_2} \rangle}\tilde{b_2} \\
&= (b_3 - \mu_{3,1}\tilde{b_1} - \mu_{3,2}\tilde{b_2}) + k(b_2 - \mu_{2,1}\tilde{b_1} - \tilde{b_2}) \\
&= \tilde{b_3} + 0
\end{aligned}$$

Correctness

For each outer loop i^{th} iteration, the reduction step ensures that the projection of b_i on $\tilde{b_j}$ for any $j < i$ is at most $\frac{1}{2}||\tilde{b_j}||$.

$$
\begin{aligned}
|\mu_{i,j}| &= \left| \frac{\langle b_i - c_{i,j} \cdot b_j, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} \right| \\
&= \left| \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} - \left\lceil \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} \right\rfloor \frac{\langle b_j, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} \right| \\
&= \left| \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} - \left\lceil \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} \right\rfloor \right| \\
&\leq \frac{1}{2}
\end{aligned}
$$

Termination I

$M = \{n, \log(\max_i ||b_i||\}$

Definition

(Potential of a lattice basis) Given a lattice basis $B = (b_1, ..., b_n)$, the potential of B is defined as

$$\begin{aligned}\mathcal{D}_b &= \prod_{i=1}^{n} ||\tilde{b_i}||^{n-i+1} \\ &= \prod_{i=1}^{n} ||\tilde{b_1}|| \, ||\tilde{b_2}|| \cdots ||\tilde{b_i}|| \\ &= \prod_{i=1}^{n} \mathcal{D}_{b,i}\end{aligned}$$

where $\mathcal{D}_{b,i} = det(\Lambda_i)$ and Λ_i is the lattice generated by vectors $b_1, ..., b_i$

Termination II

Theorem

The number of iterations is polynomial in M.

Λ_k remains the same for $k \neq i$. Thus, $\mathcal{D}_{b,k}$ also remains the same for $k \neq i$.

$$\frac{\mathcal{D}'_{b,i}}{\mathcal{D}_{b,i}} = \frac{det\Lambda'_i}{det\Lambda_i} = \frac{det\Lambda(b_1, ..., b_{i-1}, b_{i+1})}{det\Lambda(b_1, ..., b_{i-1}, b_i)}$$
$$= \frac{\left(\prod_{j=1}^{i-1} ||\tilde{b}_j||\right) ||\tilde{b}'_{i+1}||}{\prod_{j=1}^{i} ||\tilde{b}_j||}$$

Before swapping, the old value of Gram-Schmidt vector corresponding to b_{i+1} is $\tilde{b}_{i+1} = b_{i+1} - \sum_{j=1}^{i} \mu_{i+1,j}\tilde{b}_j$
After swapping new value is $\tilde{b}'_{i+1} = b_{i+1} - \sum_{j=1}^{i-1} \mu_{i+1,j}\tilde{b}_j = \tilde{b}_{i+1} + \mu_{i+1,i} \cdot \tilde{b}_i$.

Termination III

$$
\begin{aligned}
&= \frac{||\tilde{b}_{i+1} + \mu_{i+1,i} \cdot \tilde{b}_i||}{||\tilde{b}_i||} \\
&< \frac{\sqrt{\delta} \cdot ||\tilde{b}_i||}{||\tilde{b}_i||} = \sqrt{\delta}
\end{aligned}
$$

Let $\mathcal{D}_{B,0}$ be the initial value of $\mathcal{D}_b$ and it is an integer quantity, then

$$
\log_{\frac{1}{\sqrt{\delta}}} \mathcal{D}_{B,0} = \frac{\log \mathcal{D}_{B,0}}{\log \frac{1}{\sqrt{\delta}}} \leq \frac{1}{\log \frac{1}{\sqrt{\delta}}} \cdot \frac{n(n+1)}{2} \cdot \log(\max_i ||b_i||)
$$

Runtime

Theorem

The running time of each iteration is polynomial in M.

The best approximation factor LLL can offer is $\left(\frac{2}{\sqrt{3}}\right)^n$ using $\delta = \frac{1}{4} + \frac{3}{4}^{n-1}$.

Future work

- Number Theory
- Factorization algorithms
- Integer Programming
- Minkowski's theorems
- Sphere Packing

References I

[1] Peter J. Cameron. *Notes on Algebraic Structures*. https://webspace.maths.qmul.ac.uk/p.j.cameron/notes/algstr.pdf. 2006.

[2] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische annalen* 261.ARTICLE (1982), pp. 515–534.

[3] Daniele Micciancio. *CSE206A: Lattices Algorithms and Applications*. https://cseweb.ucsd.edu//classes/wi10/cse206a/. 2010.

[4] Chris Peikert. *EECS 598: Lattices in Cryptography*. https://web.eecs.umich.edu/~cpeikert/lic15/index.html. 2015.

[5] Oded Regev. *Lattices in Computer Science*. https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/. 2009.

References II

[6] Vinod Vaikuntanathan. *CSC2414: Topics in Applied Discrete Mathematics: Lattices in Computer Science*. https://people.csail.mit.edu/vinodv/COURSES/CSC2414-F11/index.html. 2011.

[7] Wikipedia contributors. *Algebraic structure — Wikipedia, The Free Encyclopedia*. [Online; accessed 6-April-2022]. 2022. URL: https://en.wikipedia.org/w/index.php?title=Algebraic_structure&oldid=1081186117.

[8] Wikipedia contributors. *Cauchy–Schwarz inequality — Wikipedia, The Free Encyclopedia*. [Online; accessed 6-April-2022]. 2022. URL: https://en.wikipedia.org/w/index.php?title=Cauchy%E2%80%93Schwarz_inequality&oldid=1072458704.

That's all folks!

Thank You!

Lattices and LLL algorithm for **MS Seminar**

Kushagra Shandilya - 21Q050010