LATTICES SEMINAR
LLL ALGORITHM

PHD STUDENT: PETRA SALA

2 OVERVIEW

1. About me
2. Summary of lattices
3. Idea of LLL
4. Lagrange-Gauss reduction basis algorithm and example
5. LLL algorithm
6. Example
7. Complexity
8. Applications
9. References

3 SUMMARY OF INTRODUCTION

- **Definition of the lattice:** Given n linearly independent vectors $b_{1,\dots}b_n \in \mathbb{R}^m$, the lattice generated by them is defined as $\mathcal{L}(b_{1,\dots}b_n) = \{\sum x_i b_i \,|x_i \in \mathbb{Z}\}$ or if $B = m \times n$ matrix whose columns are $b_{1,\dots}b_n$ then the lattice generated by B is $\mathcal{L}(B) = \mathcal{L}(b_{1,\dots}b_n) = \{Bx|x \in \mathbb{Z}^n\}$
- **Successive minima** : Let Λ be a lattice of rank n. For $i \in \{1, \dots n\}$ we define ith successive minima as $\lambda_i(\Lambda) = \inf\{r|\dim\left(span(\Lambda \cap \bar{B}(0,r))\right) \geq i\}$ where $\bar{B}(0,r) = \{x \in \mathbb{R}^m | \|x\| \leq r\}$
- **Minkowski first theorem:** For any full-rank lattice Λ of rank n, $\lambda_i(\Lambda) \leq \sqrt{n}(det\Lambda)^{\frac{1}{n}}$.
- **Minkowski second theorem:** For any full-rank lattice Λ of rank n, $(\prod_{i=1}^{n} \lambda_i(\Lambda))^{\frac{1}{n}} \leq \sqrt{n}(det\Lambda)^{\frac{1}{n}}$.

4 IDEA OF LLL

- Lenstra, Lenstra and Lovazs1982.
- Lattice basis reduction
  - Goal is to transform a given basis into a "nicer" basis that is easier to work with
  - "Nicer" basis: Basis consisting of vectors which are short and close to orthogonal
- Some of the interesting applications:
  - Approximation algorithm to the Shortest Vector Problem (SVP)
- A generalization of Lagrange-Gauss reduction of vectors in two dimensions

5 LAGRANGE-GAUSS REDUCTION ALGORITHM

- Lattice basis reductions in two dimensions
- Closely related to Euclid's algorithm
- Let $b_1, b_2 \in \mathbb{R}^2$ be linear independent vectors and Λ is a lattice in which they are basis
  - Goal : output a basis for the lattice such that the length of the basis vectors are as short as possible

Example:

$b_1 = (1,5), b_2 = (6,21)$

Algorithm 23 Lagrange-Gauss lattice basis reduction

INPUT: Basis $\underline{b}_1, \underline{b}_2 \in \mathbb{Z}^2$ for a lattice L

OUTPUT: Basis $(\underline{b}_1, \underline{b}_2)$ for L such that $\|\underline{b}_i\| = \lambda_i$

1: $B_1 = \|\underline{b}_1\|^2$
2: $\mu = \langle \underline{b}_1, \underline{b}_2 \rangle / B_1$
3: $\underline{b}_2 = \underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$
4: $B_2 = \|\underline{b}_2\|^2$
5: **while** $B_2 < B_1$ **do**
6: Swap $\underline{b}_1$ and $\underline{b}_2$
7: $B_1 = B_2$
8: $\mu = \langle \underline{b}_1, \underline{b}_2 \rangle / B_1$
9: $\underline{b}_2 = \underline{b}_2 - \lfloor \mu \rceil \underline{b}_1$
10: $B_2 = \|\underline{b}_2\|^2$
11: **end while**
12: **return** $(\underline{b}_1, \underline{b}_2)$

$B_1 = 26$

$\mu \approx 4.27$

$b_2 = b_2 - 4b_1 = (2,1)$

$B_2 = 5$

Swap

$b_1 = (2,1), b_2 = (1,5)$

Reduced basis

$\{\boldsymbol{b_1 = (2,1), b_2 = (-1,-4)}\}$

7 LLL ALGORITHM

- Full-rank matrices
- Applies on other norms
- Stages:
    1. Define Gram Schmidt Orthogonalization
    2. Define an LLL reduced basis and show some important properties
    3. Present an algorithm to find such basis
    4. Example

8 LLL ALGORITHM

- Recap Gram-Schmidt Orthogonalization
  - Definition: Given n linearly independent vectors $b_{1,\dots}b_n \in \mathbb{R}^n$, the Gram-Schmidt Orthogonalization of $b_{1,\dots}b_n$ is defined by $\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j}\tilde{b}_j$, where $\mu_{i,j} = \frac{\langle b_i | \tilde{b}_j \rangle}{\langle \tilde{b}_j | \tilde{b}_j \rangle}$.
- Definition (Reduced basis): A basis $B = \{b_{1,\dots}b_n\} \in \mathbb{R}^n$ is a $\delta - LLL\ Reduced\ Basis$ if the following holds:
  1. $\forall 1 \le i \le n, j < i, |\mu_{i,j}| \le \frac{1}{2}$
  2. $\forall 1 \le i \le n, \delta \|\tilde{b}_i\|^2 \le \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2$ **Lovazs condition**

9 PROPERTIES OF LLL

1. $\forall \mathbf{1} \leq \boldsymbol{i} \leq \boldsymbol{n}, \boldsymbol{j} < \boldsymbol{i}, \left|\boldsymbol{\mu_{i,j}}\right| \leq \frac{\mathbf{1}}{\mathbf{2}}$

- $\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}_j$, where $\mu_{i,j} = \dfrac{\langle b_i | \tilde{b}_j \rangle}{\langle \tilde{b}_j | \tilde{b}_j \rangle}$
- $b_i = \tilde{b}_i + \sum_{j=1}^{i-1} \mu_{i,j} \tilde{b}_j$ ⟶ $B = \{b_1, \dots, b_n\}$
- $\left|\boldsymbol{\mu_{i,j}}\right| \leq \frac{\mathbf{1}}{\mathbf{2}}$ ⟶

$$\begin{pmatrix} \|\tilde{b}_1\| & \leq \frac{1}{2}\|\tilde{b}_1\| & \cdots & \leq \frac{1}{2}\|\tilde{b}_1\| \\ 0 & \|\tilde{b}_2\| & \cdots & \leq \frac{1}{2}\|\tilde{b}_2\| \\ \vdots & & \ddots & \vdots \\ & & & \leq \frac{1}{2}\|\tilde{b}_{n-1}\| \\ 0 & \cdots & & \|\tilde{b}_n\| \end{pmatrix}$$

$$B = \begin{pmatrix} \|\tilde{b}_1\| & \mu_{2,1}\|\tilde{b}_1\| & \cdots & \mu_{n,1}\|\tilde{b}_1\| \\ 0 & \|\tilde{b}_2\| & \cdots & \mu_{n,2}\|\tilde{b}_n\| \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \|\tilde{b}_n\| \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

10 PROPERTIES OF LLL

$$\begin{pmatrix} \|\tilde{b}_1\| & \mu_{2,1}\|\tilde{b}_1\| & \cdots & \mu_{n,1}\|\tilde{b}_1\| \\ 0 & \|\tilde{b}_2\| & \cdots & \mu_{n,2}\|\tilde{b}_n\| \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \|\tilde{b}_n\| \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

2. $\forall 1 \leq i \leq n, \delta\|\tilde{b}_i\|^2 \leq \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2$ **Lovazs condition (size)**

- $\delta\|\tilde{b}_i\|^2 \leq \|\mu_{i+1,i}\tilde{b}_i + \tilde{b}_{i+1}\|^2 = {\mu_{i+1,i}}^2\|\tilde{b}_i\|^2 + \|\tilde{b}_{i+1}\|^2$ ➡
- $\|\tilde{b}_{i+1}\|^2 \geq (\delta - {\mu_{i+1,i}}^2)\|\tilde{b}_i\|^2 \geq (\delta - \frac{1}{4})\|\tilde{b}_i\|^2, \delta = \frac{3}{4}$
- $\|\tilde{\boldsymbol{b}}_{\boldsymbol{i}}\| \leq \boldsymbol{2^{\frac{1}{2}}}\|\tilde{\boldsymbol{b}}_{\boldsymbol{i+1}}\|$
- Remarks:
  1. It is always possible to transform a basis into a reduced basis
  2. It is usually considered $\delta = \frac{3}{4}$, but the algorithm works with any $\frac{1}{4} < \delta < 1$

11 PROPERTIES OF LLL

- Claim : Let $\{b_{1,\dots}b_n\} \in \mathbb{R}^n$ be a $\delta - LLL\ Reduced\ Basis$. Then $\|b_1\| \leq (\frac{2}{\sqrt{4\delta-1}})^{n-1}\lambda_1(L)$
- Remark: For $\delta = \frac{3}{4}$ → $\|b_1\| \leq 2^{\frac{n-1}{2}}\lambda_1(L)$
- Proof:
- For any basis $\{b_{1,\dots}b_n\}$, it holds that $\lambda_1(\Lambda) \geq min_i\|\tilde{b}_i\|$, and because $\|\tilde{\boldsymbol{b}}_{\boldsymbol{i}}\| \leq \left(\delta - \frac{1}{4}\right)\|\tilde{\boldsymbol{b}}_{\boldsymbol{i+1}}\|$, we get that
- $\|\tilde{b}_n\|^2 \geq \left(\delta - \frac{1}{4}\right)\|\tilde{b}_{n-1}\|^2 \geq \cdots \geq \left(\delta - \frac{1}{4}\right)^{n-1}\|\tilde{b}_1\|^2$, by def. $\tilde{b}_1 = b_1$
- Then for any i, $\|\tilde{b}_1\|^2 \leq \left(\delta - \frac{1}{4}\right)^{\frac{-(i-1)}{2}}\|\tilde{b}_i\|^2 \leq \left(\delta - \frac{1}{4}\right)^{\frac{-(n-1)}{2}}\|\tilde{b}_i\|^2$

12 PROPERTIES OF LLL

- $\|\tilde{b}_1\|^2 \leq \left(\delta - \frac{1}{4}\right)^{\frac{-(i-1)}{2}} \|\tilde{b}_i\|^2 \leq \left(\delta - \frac{1}{4}\right)^{\frac{-(n-1)}{2}} \|\tilde{b}_i\|^2$
- Hence, $\|b_1\| \leq (\frac{2}{\sqrt{4\delta-1}})^{n-1} min_i \|\tilde{b}_i\| \leq 2(\frac{2}{\sqrt{4\delta-1}})^{n-1^{\frac{n-1}{2}}} \lambda_1(L)$.
- Claim provides us with an approximation to the SVP problem
  - We run LLL and return b_1 as our answer

13 PROPERTIES FOR LLL

- Other nice properties:
  a) For $\forall 1 \leq i \leq n, \|b_i\| \leq 2^{\frac{i-1}{2}} \|\tilde{b}_i\|$
  b) For $\forall 1 \leq i \leq j \leq n, \|b_i\| \leq 2^{\frac{j-1}{2}} \|\tilde{b}_j\|$
  c) $\|b_1\| \leq 2^{\frac{n-1}{4}} (det\Lambda)^{\frac{1}{n}}$
  d) $\prod \|b_i\| \leq 2^{\frac{n(n-1)}{4}} det\Lambda$
- Proof: On the black board.

Algorithm 25 LLL algorithm with Euclidean norm (typically, choose $\delta = 3/4$)

INPUT: $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^m$.
OUTPUT: LLL reduced basis $\underline{b}_1, \ldots, \underline{b}_n$

Compute the Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$ and coefficients $\mu_{i,j}$ for $1 \leq j < i \leq n$
Compute $B_i = \langle \underline{b}_i^*, \underline{b}_i^* \rangle = \|\underline{b}_i^*\|^2$ for $1 \leq i \leq n$
$k = 2$
while $k \leq n$ **do**
    for $j = (k-1)$ downto 1 **do** ▷ Perform size reduction
        Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $\underline{b}_k = \underline{b}_k - q_j \underline{b}_j$
        Update the values $\mu_{k,j}$ for $1 \leq j < k$
    end for
    if $B_k \geq (\delta - \mu_{k,k-1}^2) B_{k-1}$ **then** ▷ Check Lovász condition
        $k = k + 1$
    else
        Swap $\underline{b}_k$ with $\underline{b}_{k-1}$
        Update the values $\underline{b}_k^*$, $\underline{b}_{k-1}^*$, B_k, B_{k-1}, $\mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \leq j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \leq n$
        $k = \max\{2, k-1\}$
    end if
end while

$$\mu_{k,j} = \frac{v_k \tilde{v}_j}{\tilde{v}_j \tilde{v}_j}$$

15 EXAMPLE FOR LLL

- Use LLL to find reduced basis for the lattice spanned by vectors : $v_1 = (15,23,11), v_2 = (46,15,3), v_3 = (32,1,1)$.
- Solution:
- Step 1: Find orthogonal vectors, $\widetilde{v_1}, \widetilde{v_2}, \widetilde{v_3}$.
  - $\widetilde{v_1} = v_1$
  - $\widetilde{v_2} = v_2 - \frac{v_2\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}} v_1 \approx (27.69, -13.07, -10.43)$
- Remarks:
  - Sequence of vectors does not matter
  - The vector we choose to reduce we call **working vector**
  - In practice if v_k is the working vector, we only need the G-S basis $\widetilde{v_1}, \ldots, \widetilde{v_k}$

16 EXAMPLE FOR LLL

Algorithm 25 LLL algorithm with Euclidean norm (typically, choose $\delta = 3/4$)

INPUT: $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^m$.
OUTPUT: LLL reduced basis $\underline{b}_1, \ldots, \underline{b}_n$

Compute the Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$ and coefficients $\mu_{i,j}$ for $1 \le j < i \le n$
Compute $B_i = \langle \underline{b}_i^*, \underline{b}_i^* \rangle = \|\underline{b}_i^*\|^2$ for $1 \le i \le n$
$k = 2$
while $k \le n$ **do**
    for $j = (k-1)$ downto 1 **do** ▷ Perform size reduction
        Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $\underline{b}_k = \underline{b}_k - q_j \underline{b}_j$
        Update the values $\mu_{k,j}$ for $1 \le j < k$
    end for
    if $B_k \ge (\delta - \mu_{k,k-1}^2) B_{k-1}$ **then** ▷ Check Lovász condition
        $k = k + 1$
    else
        Swap $\underline{b}_k$ with $\underline{b}_{k-1}$
        Update the values $\underline{b}_k^*$, $\underline{b}_{k-1}^*$, B_k, B_{k-1}, $\mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \le j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \le n$
        $k = \max\{2, k-1\}$
    end if
end while

- Step 2 (size reduction):
  - We use v_1 to reduce v_2
  - $v_2 = v_2 - \left[\frac{v_2 \widetilde{v_1}}{\widetilde{v_1} \widetilde{v_1}}\right] v_1 = (31, -8, -8)$
  - New $v_2 = (31, -8, -8)$
- Step 3 (checking Lovazs condition):
  - $\|\widetilde{v_1}\|^2 = 875$
  - $\|\widetilde{v_2}\|^2 \approx 1046.43$
  - $\mu_{2,1} = \frac{v_2 \widetilde{v_1}}{\widetilde{v_1} \widetilde{v_1}} = 0.221$

$$\|\widetilde{v_2}\|^2 \geq \left(\frac{3}{4} - {\mu_{2,1}}^2\right) \|\widetilde{v_1}\|^2$$

That is true and we move on to the next vector, v_3.

17 EXAMPLE FOR LLL

- New basis state:
  - $v_1 = (15,23,11), v_2 = (31,-8,-8), v_3 = (32,1,1)$
- We repeat the steps again:
  - Recomputing G-S : $\widetilde{v_1} = v_1$
  - $\widetilde{v_2} \approx (27.691, -13.073, -10.426)$
  - $\widetilde{v_3} = \frac{v_3\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}}\widetilde{v_1} - \frac{v_3\widetilde{v_2}}{\widetilde{v_2}\widetilde{v_2}}\widetilde{v_2} \approx (0.361, -1.734, -3.133)$
  - Now use v_1 to reduce v_3
  - $v_3 = v_3 - \left[\frac{v_3\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}}\right] v_1 = (17, -22, -10)$

Algorithm 25 LLL algorithm with Euclidean norm (typically, choose $\delta = 3/4$)

INPUT: $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^m$.
OUTPUT: LLL reduced basis $\underline{b}_1, \ldots, \underline{b}_n$

Compute the Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$ and coefficients $\mu_{i,j}$ for $1 \le j < i \le n$
Compute $B_i = \langle \underline{b}_i^*, \underline{b}_i^* \rangle = \|\underline{b}_i^*\|^2$ for $1 \le i \le n$
$k = 2$
while $k \le n$ **do**
    for $j = (k-1)$ downto 1 **do** ▷ Perform size reduction
        Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $\underline{b}_k = \underline{b}_k - q_j \underline{b}_j$
        Update the values $\mu_{k,j}$ for $1 \le j < k$
    end for
    if $B_k \ge (\delta - \mu_{k,k-1}^2) B_{k-1}$ **then** ▷ Check Lovász condition
        $k = k + 1$
    else
        Swap $\underline{b}_k$ with $\underline{b}_{k-1}$
        Update the values $\underline{b}_k^*$, $\underline{b}_{k-1}^*$, B_k, B_{k-1}, $\mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \le j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \le n$
        $k = \max\{2, k-1\}$
    end if
end while

18 EXAMPLE FOR LLL

Algorithm 25 LLL algorithm with Euclidean norm (typically, choose $\delta = 3/4$)

INPUT: $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^m$.
OUTPUT: LLL reduced basis $\underline{b}_1, \ldots, \underline{b}_n$

Compute the Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$ and coefficients $\mu_{i,j}$ for $1 \le j < i \le n$
Compute $B_i = \langle \underline{b}_i^*, \underline{b}_i^* \rangle = \|\underline{b}_i^*\|^2$ for $1 \le i \le n$
$k = 2$
while $k \le n$ **do**
    for $j = (k-1)$ downto 1 **do** ▷ Perform size reduction
        Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $\underline{b}_k = \underline{b}_k - q_j \underline{b}_j$
        Update the values $\mu_{k,j}$ for $1 \le j < k$
    end for
    if $B_k \ge (\delta - \mu_{k,k-1}^2) B_{k-1}$ **then** ▷ Check Lovász condition
        $k = k + 1$
    else
        Swap $\underline{b}_k$ with $\underline{b}_{k-1}$
        Update the values $\underline{b}_k^*$, $\underline{b}_{k-1}^*$, B_k, B_{k-1}, $\mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \le j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \le n$
        $k = \max\{2, k-1\}$
    end if
end while

- Now use v_2 to reduce v_3
  - $v_3 = v_3 - \left[\frac{v_3 \widetilde{v_2}}{\widetilde{v_2}\widetilde{v_2}}\right] v_2 = (-14, -14, -2)$
  - New basis state: $v_1 = (15,23,11), v_2 = (31, -8, -8), v_3 = (-14, -14, -2)$
- Checking the Lovazs condition:
  - $\|\widetilde{v_2}\|^2 \approx 1046.43$
  - $\|\widetilde{v_3}\|^2 \approx 12.954$
  - $\mu_{3,2} = \frac{v_3 \widetilde{v_2}}{\widetilde{v_2}\widetilde{v_2}} \approx -0.176$

$$\|\widetilde{v_3}\|^2 \ge \left(\frac{3}{4} - {\mu_{3,2}}^2\right) \|\widetilde{v_2}\|^2$$

That is **NOT** true and we **swap** v_3 and v_2.

19 EXAMPLE FOR LLL

- New basis state:
  - $v_1 = (15,23,11), v_2 = (-14,-14,-2), v_3 = (31,-8,-8)$
- Working vector is again v_2
- Repeat the steps:
  - Recompute G-S basis up to v_2: $\widetilde{v_1} = v_1$
  - $\widetilde{v_2} = v_2 - \frac{v_2\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}} v_1 \approx (-4.503, 0.562, 4.965)$
  - We use v_1 to reduce v_2
  - $v_2 = v_2 - \left[\frac{v_2\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}}\right] v_1 = (1,9,9)$
  - New $v_2 = (1,9,9)$

Algorithm 25 LLL algorithm with Euclidean norm (typically, choose $\delta = 3/4$)

INPUT: $\underline{b}_1, \ldots, \underline{b}_n \in \mathbb{Z}^m$.
OUTPUT: LLL reduced basis $\underline{b}_1, \ldots, \underline{b}_n$

1: Compute the Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$ and coefficients $\mu_{i,j}$ for $1 \le j < i \le n$
2: Compute $B_i = \langle \underline{b}_i^*, \underline{b}_i^* \rangle = \|\underline{b}_i^*\|^2$ for $1 \le i \le n$
3: $k = 2$
4: **while** $k \le n$ **do**
5: **for** $j = (k-1)$ downto 1 **do** ▷ Perform size reduction
6: Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $\underline{b}_k = \underline{b}_k - q_j \underline{b}_j$
7: Update the values $\mu_{k,j}$ for $1 \le j < k$
8: **end for**
9: **if** $B_k \ge (\delta - \mu_{k,k-1}^2) B_{k-1}$ **then** ▷ Check Lovász condition
10: $k = k + 1$
11: **else**
12: Swap $\underline{b}_k$ with $\underline{b}_{k-1}$
13: Update the values $\underline{b}_k^*$, $\underline{b}_{k-1}^*$, B_k, B_{k-1}, $\mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \le j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \le n$
14: $k = \max\{2, k-1\}$
15: **end if**
16: **end while**

20 EXAMPLE FOR LLL

- Checking Lovazs condition:
  - $\|\widetilde{v_1}\|^2 = 875$
  - $\|\widetilde{v_2}\|^2 \approx 45.239$
  - $\mu_{2,1} = \frac{v_2\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}} = 0.367$
- New basis state:
  - $v_1 = (1,9,9), v_2 = (15,23,11),, v_3 = (31,-8,-8)$
  - Recompute G-S basis up to v_2: $\widetilde{v_1} = v_1$
  - $\widetilde{v_2} = v_2 - \frac{v_2\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}} v_1 \approx (13.031, 5.276, -6.724)$
  - We use v_1 to reduce v_2

$$\|\widetilde{v_2}\|^2 \geq (\frac{3}{4} - {\mu_{2,1}}^2)\ \|\widetilde{v_1}\|^2$$

That is **NOT** true and we **swap** v_1 and v_2.

$$v_2 = v_2 - \left[\frac{v_2\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}}\right] v_1 = (13,5,-7)$$

New $v_2 = (13,5,-7)$

$$\|\widetilde{v_2}\|^2 \geq (\frac{3}{4} - {\mu_{2,1}}^2)\ \|\widetilde{v_1}\|^2$$

That is true and we move on to the next vector, v_3.

.

21 EXAMPLE FOR LLL

- New basis state:
  - $v_1 = (1,9,9), v_2 = (13,5,-7), v_3 = (31,-8,8)$
- We repeat the steps again:
  - Recomputing G-S : $\widetilde{v_1} = v_1$
  - $\widetilde{v_2} \approx (13.031,5.276,-6.724)$
  - $\widetilde{v_3} = \frac{v_3\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}}\widetilde{v_1} - \frac{v_3\widetilde{v_2}}{\widetilde{v_2}\widetilde{v_2}}\widetilde{v_2} \approx (9.397,-10.789,9.745)$
  - Now use v_1 to reduce v_3
  - $v_3 = v_3 - \left[\frac{v_3\widetilde{v_1}}{\widetilde{v_1}\widetilde{v_1}}\right] v_1 = (32,1,1)$

Now use v_2 to reduce v_3

$$v_3 = v_3 - \left[\frac{v_3\widetilde{v_2}}{\widetilde{v_2}\widetilde{v_2}}\right] v_2 = (6,-9,15)$$

Final basis state:

$$v_1 = (1,9,9), v_2 = (13,5,-7), v_3 = (6,-9,15)$$

$$\|\widetilde{v_2}\|^2 \approx 242.847$$

$$\|\widetilde{v_3}\|^2 \approx 299.645$$

$$\mu_{3,2} = \frac{v_3\widetilde{v_2}}{\widetilde{v_2}\widetilde{v_2}} \approx -0.289$$

$$\|\widetilde{v_3}\|^2 \geq \left(\frac{3}{4} - {\mu_{3,2}}^2\right) \|\widetilde{v_2}\|^2$$

That is true and we are done because we only have three vectors.

22 COMPLEXITY

- We measure time complexity with integer valued lattices:
- Theorem Let $\mathcal{L}$ be a lattice in $\mathbb{Z}^m$ with basis $b_{1,\dots}b_n$ and let $X \in \mathbb{Z}_{\geq 2}$ be such that $\|b_i\|^2 \leq X$ for $1 \leq i \leq n$. Let $\frac{1}{4} < \delta < 1$. Let the LLL algorithm with factor δ terminates and performs at most $\frac{1}{\log(\frac{1}{\sqrt{\delta}})} \frac{n(n+1)}{2} \log(x)$ iterations.
- Corollary Let $\mathcal{L}$ be a lattice in $\mathbb{Z}^m$ with basis $b_{1,\dots}b_n$ and let $X \in \mathbb{Z}_{\geq 2}$ be such that $\|b_i\|^2 \leq X$ for $1 \leq i \leq n$. Then the LLL algorithm requires $O(n^3 m \log(X))$ arithmetic operations on integers on size $O(n \log(X))$. Using naïve arithmetic gives running time $O(n^5 m \log(X)^3)$ bit operations.

23 IMPROVEMENTS OF LLL

- Schnorr 1987. presented improved algorithm
  - The idea is that rather than just swapping b_k and b_{k-1} in the LLL, one can move b_k much earlier in the list if B_k is sufficiently small
- Korkine-Zolotarev algorithm
- Others

24 OTHER APPLICATIONS

- Factoring polynomials over the integers or the rational numbers
- Finding the minimal polynomial of an algebraic number given to a good enough approximation
- Finding integer relations
- Integer programming
- Approximation to the Closest Vector Problem
- Breaking cryptographic protocols (e.g. low public exponent attack in RSA)

25 REFERENCES

- https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/lll.pdf
- https://cseweb.ucsd.edu/classes/wi12/cse206A-a/lec3.pdf
- https://www.youtube.com/watch?v=n5MfVR77BTw
- https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf

THANK YOU FOR YOUR ATTENTION!