Plan for today

- Lattice basis reduction
- Gaussian algorithm
- The LLL algorithm

↙ A.K.
Lenstra, Lenstra & Lovász

Minkowski:

$\exists\, v \in \Lambda(A) \setminus \{0\}$

$\|v\|_\infty \leq \sqrt[n]{\det(\Lambda)}$

Finding such a v is open problem.

Recall

Theorem
A lattice $\Lambda \subseteq \mathbb{R}^n$ has a nonzero lattice point of length bounded by $2 \cdot \sqrt[n]{\det(\Lambda)/V_n}$.

Orthogonality defect:

- $b_1, \dots, b_n$ lattice basis.
- $B = (b_1, \dots, b_n)$
- $\gamma \in \mathbb{R}$ with $|\det(B)| = \gamma \cdot \prod_{i=1}^{n} \|b_i\|$

"orthogonality defect."

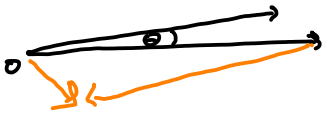
Shortest vector is of the form $B \cdot x$, $\|x\|_\infty \leq \gamma$

$(2\gamma + 1)^n$ candidates. Constant if n and γ are constant.

Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$$60^\circ \leq \phi \leq 120^\circ.$$



Definition

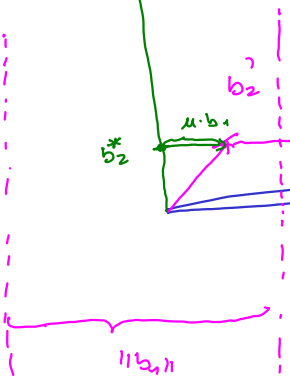
$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

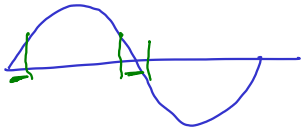
$$60° \leq \phi \leq 120°.$$

$30° \leq \phi \leq 150°$

$\left(\sin^2(\theta) + \frac{1}{4}\right) < 1/2$

$\Leftrightarrow \sin^2(\theta) < \frac{1}{4}.$





$\|b_2^*\| = b_2 \cdot \sin(\theta)$

$\|b_2'\|^2 = \|b_2^* + \mu \cdot b_1\|^2 = \|b_2^*\|^2 + \mu^2 \|b_1\|^2$

$|\mu| \leq 1/2 \;=$

b_2

b_1

$\leq \sin^2(\theta) \cdot \|b_2\|^2 + \frac{1}{4} \cdot \|b_1\|^2$

$\leq \underbrace{\left(\sin^2(\theta) + 1/4\right)}_{\leq 1} \cdot \|b_2\|^2$

$\Rightarrow (60° \leq \phi \leq 120°)$

Lagrange's algorithm:

- Each second iteration: $\|\cdot\|$ of longer vector is scaled w.r.t. $\leq 1/2$. bin. enc. length.
- # of iterations is linear in $\mathrm{Size}(b_1, b_2)$

Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$$60° \leq \phi \leq 120°.$$

Input: $b_1, b_2 \in \mathbb{R}^2$ (lin. indep).

if $\|b_2\| < \|b_1\|$ swap b_2 and b_1.

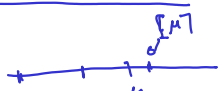
While $\sin^2(\Theta) < 1/4$.

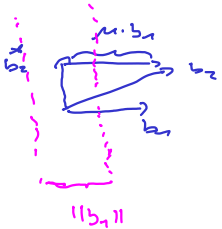
- $b_2' = b_2 - \lfloor \mu \rceil \cdot b_1$
- swap (b_1, b_2)

$\lfloor \mu \rceil$

then $b_2' = b_2^* + \lambda \cdot b_1$, w.r.t. $|\lambda| \leq 1/2$

$b_2 = b_2^* + \mu \cdot b_1$



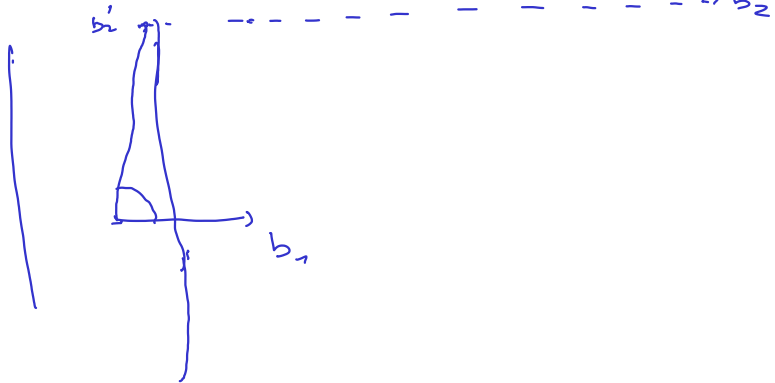


Observe that $b_2' \neq b_2$ and $b_2' \neq b_1$ unless $60° \leq \phi \leq 120°$

Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$$60^\circ \leq \phi \leq 120^\circ.$$



Reduced basis

Definition

Let $f : \mathbb{N} \to \mathbb{N}$ be a function and $B \in \mathbb{Z}^{n \times n}$ be a lattice basis. B is *f-reduced* or simply *reduced* if the orthogonality defect of B is bounded by $f(n)$.

Result of research by Lagrange, Hermite & Gauss: 19th century:

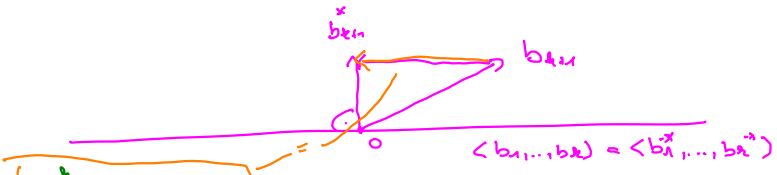
$\exists f$ such that: Each lattice $\mathcal{L}(B) \subseteq \mathbb{R}^n$ has a reduced basis.

Gram-Schmidt orthogonalization

Given: $b_1, \ldots, b_n$, computes $b_1^*, \ldots, b_n^*$ such that

i) The vectors $b_1, \ldots, b_k$ span the same subspace as $b_1^*, \ldots, b_k^*$ for each $k = 1, \ldots, n$.

ii) The vectors $b_1^*, \ldots, b_n^*$ are pairwise orthogonal.



$$b_{k+1}^* = b_{k+1} - \sum_{j=1}^{k} \mu_{j,k+1} \cdot b_j^*$$

$$\left\langle b_{k+1} - \sum_{j=1}^{k} \mu_{j,k+1} b_j^*, b_i^* \right\rangle = 0$$

for all $i = 1, \ldots, k$

$$\hookrightarrow = \langle b_{k+1}, b_i^* \rangle - \sum_{j=1}^{k} \mu_{k+1,i} \langle b_j^*, b_i^* \rangle$$

Observation: Let $b_1^*, \dots, b_i^*, b_{i+1}^*, b_{i+2}^*, \dots, b_n^*$ be the GSO of $b_1, \dots, b_i, b_{i+1}, \dots, b_n$ and let $c_1^*, \dots, c_i^*, c_{i+1}^*, \dots, c_n^*$ be GSO of $b_1, \dots, b_{i+1}, b_i, b_{i+2}, \dots b_n$. Then

$$c_k^* = b_k^* \quad \text{for } k \in \{1, \dots, i-1\} \cup \{i+2, \dots, n\}$$

Gram-Schmidt orthogonalization

Given: $b_1, \ldots, b_n$, computes $b_1^*, \ldots, b_n^*$ such that

i) The vectors $b_1, \ldots, b_k$ span the same subspace as $b_1^*, \ldots, b_k^*$ for each $k = 1, \ldots, n$.

ii) The vectors $b_1^*, \ldots, b_n^*$ are pairwise orthogonal.

$$\langle b_{k+1}, b_i^* \rangle - \sum_{j=1}^{i-1} \mu_{k+1,i} \underbrace{\langle b_j^*, b_i^* \rangle}_{=0 \text{ if } i \neq j} = \langle b_{k+1}, b_i^* \rangle - \mu_{k+1,i} \langle b_i^*, b_i^* \rangle$$

$$\Rightarrow \mu_{k+1,i} = \frac{\langle b_{k+1}, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle}.$$

q.s.o.

Lower bound on $SV(\Lambda)$

$b_1^* \leftarrow b_1$
For $j = 2, \ldots, k$
  $b_j^* \leftarrow b_j - \sum_{i=1}^{j-1} \mu_{ji} b_i^*$
  where $\mu_{ji} = \langle b_j, b_i^* \rangle / \|b_i^*\|^2$.

$\langle b_i, b_i^* \rangle$

$$b_j = \sum_{i=1}^{j-1} \mu_{ji} \cdot b_i^* + b_j^*$$

$$(b_1, \ldots, b_n) = (b_1^*, \ldots, b_n^*) \cdot \begin{pmatrix} 1 & \mu \\ & \ddots \\ 0 & & 1 \end{pmatrix}$$

R

$$B = B^* \cdot R$$

Question.

$SV(\Lambda(B))$ IF $B = B^*$. $SV(\Lambda(B))$ is shortest column of B.

Quality of Approximation

Lemma

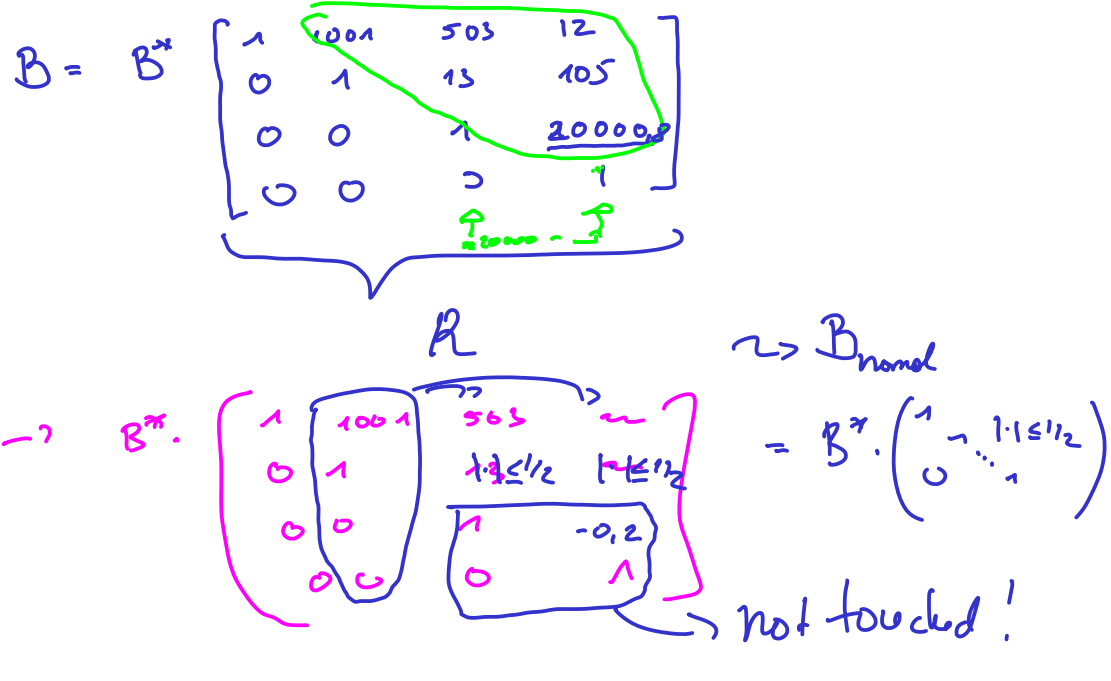
Let $B = B^* \cdot R$ be the GSO of B. The length of a shortest column of B^* is a lower bound on the length of a shortest vector of $\Lambda(B)$.

Proof: Let $v = B \cdot x$, $x \in \mathbb{Z}^n$ be a shortest vector. $x = \begin{pmatrix} x_1 \\ \vdots \\ x_k \neq 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$$v = B \cdot x = B^* \cdot \begin{bmatrix} 1 & \cdots & \mu \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} = B^* \cdot \begin{pmatrix} \sim \\ \sim \\ x_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$= \sim \cdot b_1^* + \sim b_2^* + \cdots + x_k \cdot b_k^* + 0$$

$$\Rightarrow \|v\| \geq \underbrace{|x_k|}_{\geq 1} \cdot \|b_k^*\| \geq \|b_k^*\| \geq \min_j \|b_j^*\|$$


B = B*
1001
503
12
13
105
20000,8
R
→ B_normal
→ B*.
1001
503
-0,2
= B*.
not touched!

Normalization

- Let r_{ij} be the j-th entry of the i-th row of R.
- Subtracting $\lfloor r_{ij} \rceil$ times the i-th column of R from the j-th column, the new entry r'_{ij} at position ij will satisfy $-1/2 < r'_{ij} \leq 1/2$
- Entries in a row below the i-th row of R remain unchanged.
- Thus working our way from the last to the first row, we obtain a basis $B' = B^* \cdot R'$ with

$$-1/2 < r'_{ij} \leq 1/2, \text{ for } 1 \leq i < j \leq n. \tag{10}$$

This procedure is called a *normalization step*.

The LLL-algorithm

Repeat the following two steps, as long as there exists a j, $1 \leq j \leq n-1$ with

$$\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 < 3/4\, \|b_j^*\|^2 : \tag{11}$$

- Normalize B
- Swap b_j and b_{j+1}

Analysis: Number of Swaps

The *potential* of a lattice basis B is defined as

$$\phi(B) = \|b_1^*\|^{2n} \|b_2^*\|^{2(n-1)} \|b_3^*\|^{2(n-2)} \cdots \|b_n^*\|^2 \tag{12}$$

Analysis: Number of Swaps

The *potential* of a lattice basis B is defined as

$$\phi(B) = \|b_1^*\|^{2n}\|b_2^*\|^{2(n-1)}\|b_3^*\|^{2(n-2)}\cdots\|b_n^*\|^2 \tag{12}$$

B' is basis after swap.

$$\begin{aligned}
\frac{\phi(B)}{\phi(B')} &= \frac{\|b_j^*\|^{2\cdot(n-j+1)}\|b_{j+1}^*\|^{2(n-j)}}{\|b_j'^*\|^{2\cdot(n-j+1)}\|b_{j+1}'^*\|^{2(n-j)}} \\
&= \frac{\|b_j^*\|^{2\cdot(n-j)}\|b_{j+1}^*\|^{2(n-j)}}{\|b_j'^*\|^{2\cdot(n-j)}\|b_{j+1}'^*\|^{2(n-j)}} \cdot \frac{\|b_j^*\|^2}{\|b_j'^*\|^2} \\
&= \frac{\|b_j^*\|^2}{\|b_j'^*\|^2} \\
&\geq \frac{4}{3}.
\end{aligned} \tag{13}$$

$\|b_j^*\|\|b_{j+1}^*\| = \|b_j'^*\|\|b_{j+1}'^*\|$

Potential is an integer

Let B_i be the matrix consisting of the first i columns of B. Then we have

$$\det(B_i^T \cdot B_i) = \|b_1^*\|^2 \cdots \|b_i^*\|^2 \in \mathbb{N} \tag{14}$$

Consequently we have

$$\phi(B) = \prod_{i=1}^{n} \det(B_i^T \cdot B_i) \in \mathbb{N}. \tag{15}$$

$B \in \mathbb{Z}^{n \times n}$

$\Rightarrow \phi(B) \in \mathbb{N}_{\geq 1}$

$\therefore$ # of iterations is $O(\ln(\phi(B)))$ = poly in size of B

Bounding the number of iterations

Theorem

The LLL-algorithm terminates in $O(n^2(\log n \cdot s)$ iterations, where s is the largest binary encoding length of a coefficient of $B \in \mathbb{Z}^{nn}$.

Warning

b_1^* approximates SV

Theorem

Let $B \in \mathbb{Z}^{n \times n}$ be LLL-reduced. Then

$$\|b_1\|^2 = \|b_1^*\|^2 \leq 2^{n-1} SV(\Lambda(B)).$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$