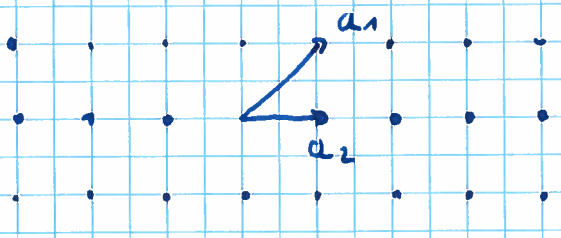
Lattices and algorithmic Geometry of Numbers.

Def: $A \in \mathbb{R}^{m \times n}$ full row-rank. non-singular. $\Lambda(A) = \{A \cdot x : x \in \mathbb{Z}^n\}$ is called vat. lattice generated by A. A is basis of lattice if $A \in \mathbb{Q}^{m \times m}$

Example: $A = (a_1, a_2) \in \mathbb{R}^{2 \times 2}$. $A = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$



Qm can see $\Lambda(A) = \Lambda\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

Def: $U \in \mathbb{Z}^{n \times n}$ is called unimodular, if

$\det(U) = \pm 1$.

Lemma: $B \in \mathbb{R}^{m \times n}$, $U \in \mathbb{Z}^{n \times n}$ unimodular.

then $\{Bx : x \in \mathbb{Z}^n\} = \{B \cdot Ux : x \in \mathbb{Z}^n\}$.

Proof: $\mathbb{Z}^n = \{U \cdot x : x \in \mathbb{Z}^n\}$.

Corollary: $A, B \in \mathbb{R}^{n \times n}$ non-singular. $\Lambda(A) = \Lambda(B) \Leftrightarrow \exists U \in \mathbb{Z}^{n \times n}$ unimod. with $A \cdot U = B$

Proof: „⇐" $\{A \cdot Ux : x \in \mathbb{Z}^n\} = \{Ax : x \in \mathbb{Z}^n\}$.

„⇒" $A \cdot X = B$, $B \cdot Y = A$ ⇒ $A \cdot X \cdot Y = A$ ⇒ $X \cdot Y = I$.

Back to example:

$$A = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \qquad A \cdot U = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

with $U = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. $\det(U) = 1$.

Algorithmic Questions:

1.) Given $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.

Find $x \in \mathbb{Z}^n$ with $A \cdot x = b$ or assert that no such x exists. (Lattice membership)

2.) Given $A \in \mathbb{Q}^{m \times n}$, $B \in \mathbb{Q}^{m \times n}$ does

$\{Ax : x \in \mathbb{Z}^n\} = \{Bx : x \in \mathbb{Z}^n\}$ hold?

(Lattice equality)

3.) Given $A \in \mathbb{Q}^{n \times n}$ lattice basis, find

$v \in \Lambda(A) \setminus \{0\}$ s.th. $\|v\|$ is minimal.

(Shortest Vector Problem)

The Hermite-Normal-Form:

Def: $B \in \mathbb{Q}^{m \times n}$ of full row-rank is in Hermite-Normal-Form (HNF), if $B = [H \mid 0]$ where H is lower triangular, non-negative, and row-maximum is on the Diagonal.

Example: $B = \begin{bmatrix} 2/3 & 0 & \cdots & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 1/2 & 1 & 0 \end{bmatrix}$

Theorem: $A \in \mathbb{Q}^{m \times n}$ full row-rank, then exists $U \in \mathbb{Z}^{n \times n}$ unimodular, s.th. $A \cdot U$ is in HNF.

Proof: Consider

$i \to \begin{pmatrix} a & b \end{pmatrix}$

$\uparrow j_1 \qquad \uparrow j_2$

not both a and b are zero. Then

$g = gcd(a,b) = x \cdot a + y \cdot b$

and $\begin{bmatrix} b/g & y \\ -a/g & x \end{bmatrix}$

is unimod.

after multiplication with

$j_1 \to \begin{pmatrix} b & b/g \end{pmatrix}$

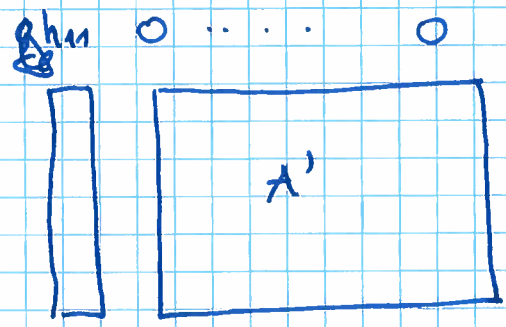
$j_2 \to \begin{pmatrix} x & -a/g \end{pmatrix}$

$\uparrow j_1 \qquad \uparrow j_2$

$\Rightarrow^{i} \to \begin{pmatrix} g & * \end{pmatrix}$

$\uparrow j_1 \qquad \uparrow j_2$

Via sequence of these operations:



Continue with A':

$$\Rightarrow \left[\begin{array}{ccc|c} h_{11} & & & \\ * & h_{22} & & \\ \times & \times & \ddots & \\ * & & * \; h_{mm} & \end{array} \;\middle|\; 0 \right]$$

Via sequence of elementary operations, reduce (*) entries modulo the diagonal elements.

Example:

$$\begin{bmatrix} 4 & 2 & 6 \\ 2 & 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\rightarrow = \begin{bmatrix} 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \ldots$$

Theorem: HNF can be computed with

$O(m \cdot n)$ gcd computations and

$O(m^2 \cdot n)$ elementary arithmetic operations.

Corollary: Every rational lattice has a basis.

Thm: ~~HNF can be computed in polytime.~~

Let $A \in \mathbb{Q}^{m \times n}$ of full row-rank.

Thm: the HNF is unique:

proof: $H = \begin{bmatrix} h_{11} & & & \\ h_{21} & h_{22} & & \\ \vdots & & \ddots & \\ h_{m1} & & & h_{mn} \end{bmatrix}$ and $H' = \begin{bmatrix} h'_{11} & & & \\ h'_{21} & h'_{22} & & \\ \vdots & & \ddots & \\ h'_{m1} & & & h'_{mm} \end{bmatrix}$

different HNFs.

We show that lattices are different.

Suppose $\Lambda(H) = \Lambda(H')$

Let i be minimal s.th. $\exists j$ with $h_{ij} \neq h'_{ij}$

W.l.o.G. assume $h'_{ij} < h_{ij}$

$G = \{ x \in \mathbb{Z} : \exists v \in \Lambda \text{ with } v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x \\ * \\ \vdots \\ * \end{pmatrix} \} \leftarrow j-1$ is $\trianglelefteq \mathbb{Z}$.

IN FACT $G = \langle h_{ii} \rangle = \langle h'_{ii} \rangle$.

But $\underbrace{h_{ij} - h'_{ij}}_{>0} \in G$ $\underbrace{< h_{ii}}$ ↯.

□.

Corollary: $\Lambda \leq \mathbb{Q}^m$ rational lattice, $\exists$ unique $H \in \mathbb{R}^{m \times m}$ in HNF with $\Lambda = \Lambda(H)$.

Thm: HNF can be computed in polynomial time.

Proof: $A \in \mathbb{Z}^{m \times n}$. D = det of m lin. indep. cols of A.

$$\Lambda(A) = \Lambda(A \mid D \cdot I)$$

$$\left[\begin{array}{c|c|ccc} H & 0 & D & & \\ & & & \ddots & \\ & & & & D \end{array}\right]$$

keep entries reduced mod D

$$\left[\begin{array}{c|c|ccc} \begin{matrix} h_{11} & & \\ h_{21} & h_{22} & \\ & & \ddots \\ h_{m1} & & h_{mm} \end{matrix} & 0 & D & & \\ & & & \ddots & \\ & & & & D \end{array}\right]$$

$$\rightarrow \left[\begin{array}{c|c|ccc} \begin{matrix} h'_{11} & & \\ x & & \\ \vdots & & \\ x & & \end{matrix} & 0 & 0 & & \\ & & D & \ddots & \\ & & & & D \end{array}\right]$$