Plan for today

- Solve the lattice membership problem
- via polynomial-time algorithm to compute Herminte Normal Form (HNF)
- Outlook on lattice basis reduction

Given: $A \in \mathbb{Z}^{m \times n}$, $v \in \mathbb{Z}^{n}$.

decide $v \in \Lambda(A)$

Solve: $A \cdot x = v$, $x \in \boxed{\mathbb{Z}^{n}}$

different from linear Alg. over $\mathbb{Q}$.

Recap: Lattices

- A *lattice* is a set $\Lambda = \{y \in \mathbb{R}^n \colon y = Ax, \ \underline{x \in \mathbb{Z}^n}\}$, where $A \in \mathbb{R}^{m \times n}$ is of full row-rank. If $A \in \mathbb{Q}^{m \times n}$, then Λ is *rational*

$\Lambda(A) = \{A \cdot x : x \in \mathbb{Z}^n\}$

- Membership problem: Given $A \in \mathbb{Q}^{m \times n}$ and $v \in \mathbb{Q}^m$, decide whether $v \in \Lambda(A)$.

The equation $ax + by = c$

G.F. Gauss, Disquisitiones Arithmeticae

$x, y \in \mathbb{Z}$

Theorem

Let a, b and c be integers. The system

$$ax + by = c \tag{2}$$

has a solution with integers x and y if and only if $\gcd(a, b) \mid c$.

proof: "⇒" Let $x^*, y^* \in \mathbb{Z}$ be a sol. $a \cdot x^* + b\, y^* = c$.

$\gcd(a,b) = d \mid a, b.$ $a = a' \cdot d$, $b = b' \cdot d$ with $a', b' \in \mathbb{Z}$.

$$d\,(a' \cdot x^* + b' \cdot y^*) = c \Rightarrow d \mid c$$

"⇐" $\exists\, \tilde{x}, \tilde{y} \in \mathbb{Z}$ s.th. $\tilde{x} \cdot a + \tilde{y} \cdot b = d$ & since $d \mid c$, $d \cdot c' = c$ for some $c' \in \mathbb{Z}$.

so $x = \tilde{x} \cdot d'$, $y = \tilde{y} \cdot d'$ is a solution. ∎

The Hermite Normal Form (HNF)

$A \in \mathbb{Q}^{\overset{m\times n}{\cancel{mn}}}$ of full row rank is said to be in *Hermite normal form (HNF)* if it has the form $[B \mid 0]$, where B is a nonsingular, nonnegative lower triangular matrix, in which each row has a unique maximal entry, located on the diagonal.

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 0 \end{pmatrix}$$

A is in HNF.

<u>Recall:</u> $A \in \mathbb{Q}^{m\times n}$, $U \in \mathbb{Z}^{n\times n}$ unimodular, then

$$\Lambda(A) = \Lambda(A \cdot U)$$

<u>Goal for today:</u> $\exists$ unimod. $U \in \mathbb{Z}^{n\times n}$ s.t. $A \cdot U$ is in HNF.

($A \in \mathbb{Q}^{m\times n}$ of full row rank)

The equation $ax + by = c$

$\underline{A = (a, b)}$, $a, b \in \mathbb{Z}$. not both zero | $A \begin{pmatrix} x \\ y \end{pmatrix} = c$ (System to solve)

$(\gcd(a,b), 0)$ is HNF of A

$\exists x, y \in \mathbb{Z}$: $\boxed{x \cdot a + y \cdot b = \gcd(a,b)}$

$A \cdot U = (\gcd , 0)$, $U = \begin{bmatrix} x & -b/\gcd \\ y & a/\gcd \end{bmatrix}$

$\det(U) = 1 \Rightarrow U$ unimod.

$$\begin{pmatrix} 4 & \boxed{3} & 2 \\ -8 & 9 & 1 \end{pmatrix} \cdot \begin{bmatrix} 1 & -3 & 0 \\ -1 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \begin{pmatrix} \boxed{\dagger} & 0 & 0 \\ & \boxed{\dagger} & \text{Rip} \end{pmatrix}$$

$$\downarrow$$

$$4 \cdot 1 + (-1) \cdot 3 = 1$$

$$U = \begin{bmatrix} x & -b/\gcd \\ y & a/\gcd \end{bmatrix}$$

$$\begin{pmatrix} 1 & 0 & \boxed{2} \\ -17 & 60 & 1 \end{pmatrix} \qquad \begin{bmatrix} -1 & 0 & -2 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$5 = 3 \cdot 60 + (-5)\, 35$$

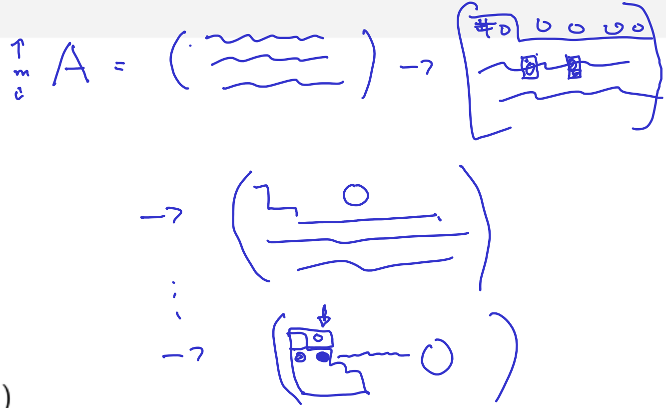
$$\downarrow \quad \downarrow \quad \downarrow$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 18 & \boxed{60} & \boxed{35} \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & -7 \\ 0 & -5 & 12 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & \boxed{0} & 0 \\ \boxed{18} & \boxed{5} & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 3 & 5 & 0 \end{bmatrix}$$

Algorithm

Input: $A \in \mathbb{Z}^{\overset{m \times n}{\cancel{mn}}}$ full row rank
Output$[H \mid 0] \in \mathbb{Z}^{mn}$ HNF of A

```
$H := A, U := I_n$
For $i = 1$ to $m$
    For $j = i + 1$ to $n$
        If $H_{i,j} \neq 0$
            $(g, x, y) = \textbf{exggT}(H_{i,i}, H_{i,j})$
            update columns $i$ and $j$ of $H$ and $U$ with $\begin{pmatrix} x & -H_{i,j}/g \\ y & H_{i,i}/g \end{pmatrix}$
    For $j = 1$ to $i - 1$   ($H_{i,i} = 0$, not possible)
        $H_{i,j} = q \cdot H_{i,i} + r$ (division with remainder)
        update columns $j$ and $i$ of $H$ and $U$ with $\begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$
```



\# steps.

$O(m^2 \cdot n)$

Theorem

Theorem

Each rational matrix $A \in \mathbb{Q}^{\overset{m \times n}{\cancel{mn}}}$ *of full row-rank can be brought into Hermite normal form by a finite series of elementary column operations.*

Proof: See Previous Alg.

Example

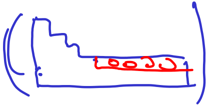
$\begin{pmatrix} 2 & 3 & 4 \\ 2 & 4 & 6 \end{pmatrix}$.

The greatest common divisor of $(2, 3)$ is $1 = (-1) \cdot 2 + 1 \cdot 3$.

Update column 1 and 2 with the matrix $\begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}$, obtaining $\begin{pmatrix} 1 & 0 & 4 \\ 2 & 2 & 6 \end{pmatrix}$.

The transforming matrix U becomes $\begin{pmatrix} -1 & -3 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

$A \cdot \underline{U} =$



Example

Eliminating 4 yields $H = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 2 & 2 & -2 \end{smallmatrix}\right)$ and $U = \begin{pmatrix} -1 & -3 & 4 \\ 1 & 2 & -4 \\ 0 & 0 & 1 \end{pmatrix}$.

Example

Eliminating -2 yields $H = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \end{smallmatrix}\right)$, $U = \begin{pmatrix} -1 & -4 & 1 \\ 1 & 4 & -2 \\ 0 & -1 & 1 \end{pmatrix}$

Example

Now reducing 2 in the lower left corner yields the Hermite normal form $H = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{smallmatrix}\right)$ and the unimodular matrix transformation matrix $U = \begin{pmatrix} 3 & -4 & 1 \\ -3 & 4 & -2 \\ 1 & -1 & 1 \end{pmatrix}$ with $A \cdot U = H$.

HNF is unique

$A \cdot U = [B \mid 0]$ $\qquad A' \cdot U' = [B' \mid 0]$

U: unimod. $\qquad [B \mid 0]$: in HNF

Lemma

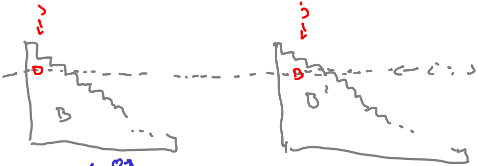
Two latttices $\Lambda(A)$ and $\Lambda(A')$ are equal, if and only if the $B = B'$, where B and B' are the lower triangular matrices in the HNFs of A and A'.

proof: Suppose $B = B'$. Then since $\Lambda(A) = \Lambda(A \cdot U) = \Lambda([B \mid 0])$

$= \Lambda(B) = \Lambda(B') = \Lambda([B' \mid 0]) = \Lambda(A')$.

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

assume $B \neq B'$. To show $\Lambda(A) \neq \Lambda(A')$ equivalently $\Lambda(B) \neq \Lambda(B')$



i: smallest row-index with a difference

Assume w.l.o.g.

$0 \leq b'_{ij} < b_{ij} < b_{ii}$

$b_j - b'_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_{ij} - b'_{ij} \\ \vdots \end{pmatrix} \in \Lambda(B)$ $\quad$ (first $i-1$ entries 0)

$\Lambda(B) = \{ B \cdot x \ ; \ x \in \mathbb{Z}^m \}$

if $v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ z \end{pmatrix} \Big\} i-1 \in \Lambda(B)$, then $z \in b_{ii} \cdot \mathbb{Z}$

↯ $0 \leq b_{ij} - b'_{ij} < b_{ii}$

HNF is unique

Lemma

~~*Two latttices $\Lambda(A)$ and $\Lambda(A')$ are equal, if and only if the $B = B'$, where B and B' are the lower triangular matrices in the HNFs of A and A'.*~~

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 4 & 3 & 0 & 0 \\ 2 & 0 & 5 & 0 \\ 4 & 1 & 3 & 12 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_3 \cdot 5 \\ x_3 \cdot 3 + x_4 \cdot 12 \end{pmatrix}$$

Towards a polynomial-time algorithm to compute the HNF

each column of $D \cdot I_m$ is in $\Lambda(A)$

$(\Leftarrow)$

Lemma

Let $A \in \mathbb{Q}^{m \times n}$ be of full row-rank and let $\Lambda(D \cdot I_m) \subseteq \Lambda(A)$, then the lower triangular matrices in the HNFs of A and $[A \mid D \cdot I_m]$ are the same.

Proof: Let $v \in \Lambda(A)$, then $\Lambda(A) = \Lambda([A \mid v])$

„$\subseteq$" trivial.

„$\supseteq$" $u \in \Lambda([A \mid v])$. $u = \underbrace{\underbrace{A \cdot x}_{\in \Lambda(A)} + \underbrace{v \cdot y}_{\in \Lambda(A)}}_{\in \Lambda(A)}$, $x \in \mathbb{Z}^n$, $y \in \mathbb{Z}$.

$\blacksquare$

A polynomial time HNF-algorithm

1. Given: $A \in \mathbb{Z}^{m \times n}$ of full row-rank
2. Compute $D \in \mathbb{N}$ with $\Lambda(D \cdot I_m) \subseteq \Lambda(A)$
3. Compute the HNF of $[A \mid D \cdot I_m]$ keeping the entries reduced $\pmod D$

$$\left[B \mid 0\right]$$

A polynomial time HNF-algorithm

1. Given: $A \in \mathbb{Z}^{m \times n}$ of full row-rank
2. Compute $D \in \mathbb{N}$ with $\Lambda(D \cdot I_m) \supseteq \Lambda(A)$
3. Compute the HNF of $[A \mid D \cdot I_m]$ keeping the entries reduced $\pmod D$

How to find such a D?

$c_1, \dots, c_m$

1.) identify m linearly independent columns of A

$\rightarrow \quad C \in \mathbb{Z}^{m \times m}$

2.) $D = |\det(C)| \qquad C \cdot \mathrm{Adj}(C) = D \cdot I_m$

$\Rightarrow$ each col. of $D \cdot I_m$ is $\in \Lambda(C) \subseteq \Lambda(A)$.

Exercise

Show that one can compute the unimodular transformation matrix $U \in \mathbb{Z}^{n \times n}$ in polynomial time as well. You may assume that Gaussian Elimination and inverse-computation can be carried out in polynomial time.

Exercise: Design a poly-time Algorithm to find a solution of

$A \cdot x = b$, $x \in \mathbb{Z}^n$, where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$.

Task: find out whether $A\cdot x = b, x\in\mathbb{Z}^n$ $(*)$. $A\in\mathbb{Z}^{m\times n}$, $b\in\mathbb{Z}^m$ has a solution or not. How to prove that $Ax=b$ does not have a sol.

Lemma: $(*)$ does not have a sol. $\Leftrightarrow$ $\exists\, y\in\mathbb{Q}^m$ s.th. $y^T\cdot A\in\mathbb{Z}^n$
$y^T\cdot b\notin\mathbb{Z}$

proof: "$\Leftarrow$" trivial. if $x^*\in\mathbb{Z}^n$ is sol. then

$$\underbrace{\underbrace{y^T\cdot A}_{\in\mathbb{Z}^n}\cdot\underbrace{x^*}_{\in\mathbb{Z}^n}}_{\in\mathbb{Z}} = \underbrace{y^T\cdot b}_{\notin\mathbb{Z}} \quad \lightning$$

"$\Rightarrow$" Assume that $Ax=b$ does have full col. rank.

$$A\cdot U = \Big(\overbrace{\boxed{B}\;\Big|\;0}^{n}\Big)\Big\}m$$

$B\cdot x=b$ has unique sol. $x^*\in\mathbb{Q}^m$.

$\cancel{(*)}$ $x^*\notin\mathbb{Z}^m$ Suppose $x_i^*\notin\mathbb{Z}$.

Finish proof in exercise. $\blacksquare$

y^T: i-th row of B^{-1}

$y^T\cdot A\in\mathbb{Z}^n$

$y^T\cdot b\notin\mathbb{Z}$.

The geometry of numbers: Minkowski's theorem

Theorem

Let $K \subseteq \mathbb{R}^n$ be a convex body which is symmetric around the origin ($x \in K$ implies $-x \in K$). If $\mathrm{Vol}(K) \geq 2^n$, then K contains a nonzero integral vector $v \in \mathbb{Z}^n \setminus \{0\}$.

Minkowski's theorem: Lattice version

Theorem

Let $\Lambda \subseteq \mathbb{R}^n$ *be a lattice and let* $K \subseteq \mathbb{R}^n$ *be a convex body of volume* $\mathrm{Vol}(K) > 2^n \det(\Lambda)$ *that is symmetric about the origin. Then* K *contains a nonzero lattice point.*

Short vectors

Theorem

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

[1]

---

[1] One has $V_n = \frac{\pi^{\lfloor n/2 \rfloor} 2^{\lceil n/2 \rceil}}{\prod_{0 \leq 2i \leq n}(n-2i)}$. Using Stirling's formula ($n! \approx \sqrt{2\,\pi\,n}\,\left(\frac{n}{e}\right)^n$) one sees that this is roughly $\left(\frac{2\pi e}{n}\right)^{n/2}$. The bound of the theorem Theorem is thus roughly $\sqrt{\frac{2}{\pi\,e}\,n}\det(\Lambda)^{1/n}$.