4.1

Prop: Λ lattice, $v_1, \dots, v_k \in \Lambda$, lin. independent, $L = \text{lin}(v_1, \dots, v_k)$
Then there is $v \in \Lambda \setminus L$, $x \in L$ s.th. $d(v,x) \leq d(w,y)$ $\forall w \in \Lambda \setminus L, y \in L$

$\longrightarrow$ use compactness of a ball around $\overline{\Pi}$ to turn this into a finite problem and enumerate

proof: Let $\overline{\Pi} := \overline{\Pi}(v_1, \dots, v_d)$

Let $a \in \Lambda \setminus L$ and $r := d(a, \overline{\Pi})$

Then
$$B_r(a) := \{ x \in \mathbb{R}^d \mid d(x, \overline{\Pi}) \leq r \}$$
is compact and $(B_r(a) \setminus L) \cap \Lambda$ is finite and not empty

$\Rightarrow$ we can choose $v \in (B_r(a) \setminus L) \cap \Lambda$ and $x \in \overline{\Pi}$ realizing
$$d(v,x) = d(v, \overline{\Pi})$$

Let $w \in \Lambda \setminus L$, $y \in L$, $\overline{\Pi} := \overline{\Pi}(v_1, \dots, v_k)$
$$\Rightarrow y = \sum \lambda_i v_i = \underbrace{\sum \lfloor \lambda_i \rfloor v_i}_{=: z \in \Lambda} + \underbrace{\sum \{ \lambda_i \} v_i}_{=: z' \in \overline{\Pi}}$$

so
$$d(w,y) = d(\underbrace{w - z}_{\in \Lambda}, \underbrace{y - z}_{\in \overline{\Pi}})$$

$\boxtimes$

With this observation we can continue to construct our lattice basis:

Choose $u_k \in \Lambda \setminus L_{k-1}$ closest to L_{k-1}

Claim: $u_1, \dots, u_k$ is a lattice basis for $L_k \cap \Lambda$

4.2

$k=1$: ✓

$k>1$: Let $v = \sum \mu_i b_i \in L_k \cap \Lambda$
$u_k = \sum \eta_i b_i$ $\Big\}\ \mu_i, \eta_i \in \mathbb{R}$

we can assume that $\mu_i, \eta_i \geq 0$ (flipping does not change distance)

choose $l \in \mathbb{Z}_{\geq 0}$ s.th.

$$v' := v - l u_k = \sum_{i=1}^{k} \mu_i' b_i \quad \text{and} \quad 0 \leq \mu_k' < \eta_k$$

$$\Rightarrow \operatorname{dist}(v', L_{k-1}) = \operatorname{dist}(\mu_k' b_k, L_{k-1})$$
$$= \mu_k' \operatorname{dist}(b_k, L_{k-1})$$
$$< \eta_k \operatorname{dist}(b_k, L_{k-1})$$
$$= \operatorname{dist}(u_k, L_{k-1})$$

Now $v' \in \Lambda$ and closer to L_{k-1} as u_k $\Rightarrow v' \in \Lambda \cap L_{k-1}$

By induction:
$$v' = \sum_{i=1}^{k-1} \lambda_i u_i \quad \text{for } \lambda_i \in \mathbb{Z}$$
$$\Rightarrow v = l u_k + \sum_{i=1}^{k-1} \lambda_i u_i \quad \text{generated by } u_1, \dots, u_k$$

This proves

Thm Every lattice has a basis. ∎

4.3

Given two bases B, B' of a lattice,
we can represent each basis vector of B as an integral linear combination of B' and vice versa,
so writing the bases as columns of two matrices B, B':

$$B = B' \cdot S \ , \ B' = B \cdot T \quad \text{with } S, T \text{ integral}$$

$$\Rightarrow B = B T S \quad \rightarrow \quad TS = \mathbb{1} \ , \text{ so } \ |\det T| = |\det S| = 1$$

This implies that $|\det B| = |\det B'|$
We define

Def: Λ lattice with basis B. Then

$$\det \Lambda := \det B = \operatorname{vol} \Pi(B)$$

is the <u>determinant</u> of Λ

The construction of a basis in the theorem is not unique.
$\rightsquigarrow$ given two bases B, B', can we decide wether $\Lambda(B) = \Lambda(B')$?

We can use more generally any finite set $B = \{b_1, \dots, b_m\} \subseteq \mathbb{R}^d$
to generate $\quad \Lambda(B) := \{ \sum \lambda_i b_i \mid \lambda_i \in \mathbb{Z} \}$

This is not necessarily a lattice (why?)

If $\Lambda(B)$ is a lattice, can we compute a basis?

$\rightsquigarrow$ need some kind of normal form (computation)
$\longrightarrow$ Hermite normal form (HNF)

The computation of the HNF is similar to Gauß elimination, but uses unimodular transformations to preserve the lattice.

$\rightsquigarrow$ search for unimodular T s.th. we can read off basis for BT

What are transformations that preserve the lattice?

(1) multiply column by -1: $T = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$

(2) swap columns i and j:

$$\begin{array}{c c} \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & 1 & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & 1 & & & 0 & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \leftarrow j \\ \\ \\ \\ \end{array} \\ \begin{array}{ccc} \uparrow & & \uparrow \\ i & & j \end{array} & \end{array}$$

(3) add k times the j-th column to the i-th column

$$\begin{array}{c c} \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & k & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \\ \\ \leftarrow j \\ \\ \\ \end{array} \\ \begin{array}{c} \uparrow \\ i \end{array} & \end{array}$$

Def: $H \in \mathbb{R}^{d \times n}$ with full row rank d is in Hermite normal form if

(1) $h_{ij} = 0$ for $j > i$

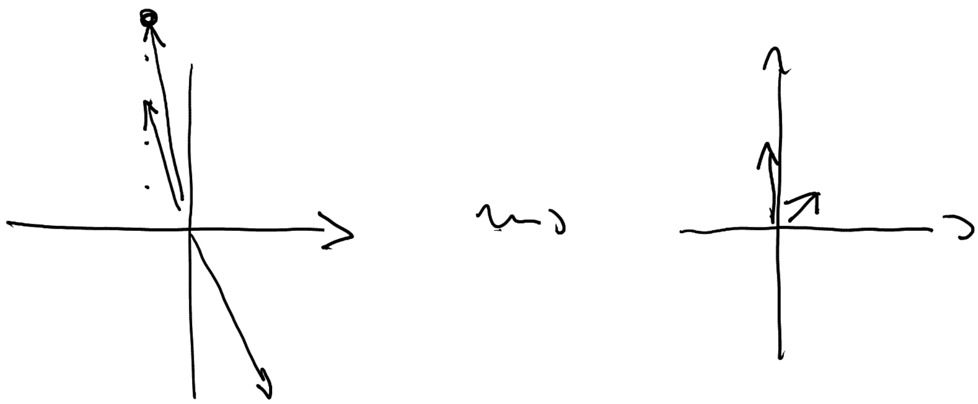
(2) $0 \le h_{ij} < h_{ii}$ for $j < i$

4.5

Thm: $A \in \mathbb{Q}^{d \times m}$. Then there is a unimodular transformation T s.th. $H = AT$ is in HNF

Example:

$$\begin{pmatrix} -1 & -1 & 2 \\ 5 & 3 & -4 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$



proof: Let q be the common denominator of the entries of A.

if H is an HNF of qA, then $\frac{1}{q} H$ is an HNF for A

$\rightsquigarrow$ it suffices to consider integer matrices A

We now prove this by induction over the rows of A:

Assume A has already the form

$$A = \begin{pmatrix} B & 0 \\ D & C \end{pmatrix}$$

with $B \in \mathbb{Z}^{k \times k}$, $k \geq 0$ in HNF

Let $(c_{11}, \dots, c_{1m-k})$ be the first row of C

with our elementary column transformations we can transform C s.th.

(1) $c_{11} \geq c_{12} \geq \dots \geq c_{1,m-k} \geq 0$

(2) $c := c_{11} + c_{12} + \dots + c_{1m-k}$ is as small as possible

then: • $c_{11} > 0$ as A has full row rank

• $c_{12} = 0$ as otherwise we can subtract second from first column (and possibly reorder)

$\Rightarrow c_{12} = c_{13} = \dots c_{1,m-k} = 0$

the column operations extend to A without affecting B, N.

$\rightsquigarrow$

$$A = \begin{array}{c} \left[\begin{array}{ccc} B & 0 & 0 \\ m & c_{11} & 0 \\ N & c' & C' \end{array}\right] \\ \begin{array}{ccc} \underbrace{\quad}_{k} & \uparrow_{k+1} & \end{array} \end{array}$$

we can use $(k+1)$st column to adjust m s.th. all entries are nonnegative and smaller than c_{11} $\boxtimes$

Prop: The HNF of a matrix is unique (no proof)

We can use the HNF to solve several lattice problems:

(1) given any $b_1, \dots, b_m \in \mathbb{Q}^n$, find a lattice basis

(2) given bases B, B', check if

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

(3) give bases B, B', find the smallest lattice containing both $\Lambda(B)$ and $\Lambda(B)$

$\rightsquigarrow$ compute $HNF(B \mid B')$

(4) containment / membership:

B, B' bases : $\Lambda(B') \subseteq \Lambda(B) \iff HNF(B \mid B') = HNF(B)$

$v \in \Lambda(B)$: $HNF(B \mid v) = HNF(B)$

<u>Remark</u> Efficient computation of the HNF:

transform first row of C:

(1) swap a column with nonzero first element to first column, make c_{11} positive

(2) for all columns c_j with nonzero first element:

compute $\gcd(c_{11}, c_{1j}) = x c_{11} + y c_{1j}$

Replace first column with

$$x c_1 + y c_j$$

j-th column with

$$\frac{1}{g}(c_{1j} c_1 - c_{11} c_j)$$

Thm: We can compute the HNF in polynomial time ☒