Prop: $\Lambda \subseteq \mathbb{R}^d$ lattice with basis $v_1, \dots, v_d$ and GS-orthogonalization $w_1, \dots, w_d$.

Then
$$\|u\| \geq \min_i (\|w_i\|) \quad \text{for all } u \in \Lambda \setminus \{0\}$$

Proof Let
$$u = \sum_{i=1}^{d} \mu_i w_i \quad \text{and} \quad k := \max_i \mu_i \neq 0$$

Then $|\mu_k| \geq 1$ and

$$\|u\| \geq |\mu_k| \|w_k\| \geq \|w_k\| \qquad \square$$

Def: The orthogonality defect of Λ is
$$\eta := \frac{1}{\det \Lambda} \prod_{i=1}^{d} \|v_i\|$$

Note $v_1, \dots, v_d$ orthogonal $\iff \eta = 1$

Def: $v_1, \dots, v_d$ is a reduced basis if the orthogonality defect is bounded by a constant η_d depending only on the dimension d.

Thm Λ lattice with reduced basis $v_1, \dots, v_d$
$u \in \Lambda \setminus \{0\}$ shortest lattice vector. Then

$$u = \sum_{j=1}^{d} \lambda_j v_j \quad \text{with} \quad |\lambda_j| \le \sqrt{d}\, \eta$$

proof Assume v_1 shortest among $v_1, \dots, v_d$

Let $V = \begin{pmatrix} | & | & & | \\ v_1 & v_2 & \cdots & v_d \\ | & | & & | \end{pmatrix}$, then $u = V\lambda$

$$\Rightarrow \lambda = V^{-1} u$$

Cramer's rule: entry q_{ij} of V^{-1} is $\dfrac{\det ij\text{-minor of } V}{\det V}$

$$\Rightarrow q_{ij} \text{ is bounded by } \|v_2\| \cdot \dots \cdot \|v_d\| \frac{1}{\det V} \le \frac{\eta}{\|v_1\|}$$

$$\Rightarrow |\lambda_j| \le \sum |u_i| \frac{\eta}{\|v_1\|} \le \sqrt{d}\, \|u\| \frac{\eta}{\|v_1\|} \le \sqrt{d}\, \eta$$

□

Now: Assume (1) there is a constant η_d bounding η independent of Λ

(2) we can find a reduced basis in polynomial time

Then we can solve (SVP) by computing a reduced basis and enumerating over all $(2\sqrt{d}\,\eta)^d$ possible shortest vectors

17. Short Lattice Bases

We still need to show that reduced bases exist and can be computed in polynomial time.

→ we look at a special case of reduced basis

Def: Λ lattice, basis $v_1, \dots, v_d$, GS-orthogonalization

$$\omega_k := v_k - \sum_{j=1}^{k} \lambda_{j,k}\, \omega_j \qquad \lambda_{j,k} := \frac{\langle v_k, \omega_j \rangle}{\|\omega_j\|^2}$$

(1) $\lambda_{j,k}$ is <u>weakly reduced</u> if $|\lambda_{j,k}| \le \frac{1}{2}$

(2) $v_1, \dots, v_d$ is — " — if all $\lambda_{j,k}$ are weakly reduced

(3) The basis is <u>δ-reduced</u> for some $\frac{1}{4} < \delta < 1$ if

(a) it is weakly reduced

(b) for all $1 \le j \le d-1$

$$\delta\, d(V_k, V_{k-1})^2 \le d(V_{k+1}, V_{k-1})^2$$

→ we only consider this for $\delta = \frac{3}{4}$.

→ Geometrically, $v_1, \dots, v_d$ is δ-reduced if v_{k+1} is "not much closer" to the subspace V_{k-1} than v_k

For an oth. basis we can recode $d(w_k, V_{k-1})$ weakly increases.

For a reduced basis we want this at least up to a factor $\sqrt{d}$

Example $V = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & 3 \end{pmatrix}$ $W = \begin{pmatrix} 2 & -\frac{2}{5} & 1 \\ 1 & 4/5 & -2 \\ 0 & 1 & 2 \end{pmatrix}$

$W = V \begin{pmatrix} 1 & -\frac{2}{5} & -\frac{1}{5} \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ ← not weakly reduced

and $d(v_1, \{0\})^2 = 5$

$d(v_2, \{0\})^2 = 2$

$\frac{3}{4}\sqrt{5} = \frac{15}{5} > 2$

violates (2)

On the other hand

$$V = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 1 & -2 \\ 1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 1/2 & -2 \\ 1 & -1/2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1/2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is $\frac{3}{4}$-reduced.

Show first that such a basis is reduced in the sense of the previous section.

For $v_i = w_i + \sum \lambda_{ij} w_j$ and $|\lambda_{ij}| \le \frac{1}{2}$ we get

$$\|w_i\|^2 \le \|v_i\|^2 \le \|w_i\|^2 + \frac{1}{4}\sum_{k=1}^{i-1} \|w_k\|^2$$

Further:

δ-reduced

$$\frac{3}{4}\|w_i\|^2 = \frac{3}{4} d(v_i, v_{i-1})^2 \le d(v_{i+1}, v_{i-1})^2 = \|w_{i+1}\|^2 + |\lambda_{i+1,i}|^2 \|w_i\|^2$$

$$\le \|w_{i+1}\|^2 + \frac{1}{4}\|w_i\|^2$$

so

$$\|w_i\|^2 \le \delta \|w_{i+1}\|^2$$

we get

$$\|v_i\|^2 \le \|w_i\|^2 + \frac{1}{4}\sum_{k=1}^{i-1} \|w_k\|^2 \le \|w_i\|^2\left(1 + \frac{1}{4}\sum_{k=1}^{i-1} \delta^{i-k}\right)$$

$$\le \delta^{i-1}\|w_i\|^2$$

So $$\frac{d}{\prod_{i=1}} \|v_i\| \le \frac{d}{\prod_{i=1}} \delta^{i-1}\|w_i\| \le \delta^{\frac{d(d-1)}{2}} \prod \|w_i\|^2$$

$$\le \delta^{\frac{d(d-1)}{2}} (\det \Lambda)^2$$

Prop: The orthogonality defect of a $\frac{3}{4}$-reduced basis is bounded by $\Pi = \delta^{\frac{d(d-1)}{2}}$.

∎

18.6

Here is a method to turn a given lattice basis into a reduced one.

→ due to Arjen Lenstra, Hendrik Lenstra, László Lovász 1982
LLL-algorithm.

Let $v_1, \dots, v_d$ be given and compute $\omega_1, \dots, \omega_d$, λ_{jk}, V_j

If $|\lambda_{jk}| > \frac{1}{2}$ for some j, k, then

$$\lambda_{ik} = a_{jk} + \mu_{jk} \quad \text{for } a_{jk} \in \mathbb{Z},\ |\mu_{jk}| \leq \frac{1}{2}$$

Set $v_k' := v_k - a_{jk} v_j$, $v_i' := v_i$ for $i \neq k$

Then:

- $V' := (v_1', \dots, v_d')$ is a lattice basis
- V_i does not change for $1 \leq i \leq d$
- $\omega_1, \dots, \omega_d$ do not change
- $\lambda_{il}' = \lambda_{il}$ for $l \neq k$ or $i > k$

Compute λ_{ik}' for $1 \leq i \leq k$:

$$v_k' = v_k - a_{jk} v_j = \omega_k + \sum_{i=1}^{k-1} \lambda_{ik} \omega_i - a_{jk} v_j$$

$v_j \in V_{j-1} = \operatorname{span}(\omega_1, \dots, \omega_{j-1})$

$$= \text{———} + \text{———} - a_{jk} \sum_{i=1}^{j} \eta_i \omega_i$$

$$= \omega_k + \sum_{i=1}^{j} (\lambda_{ik} + a_{jk} \eta_i) \omega_i + \sum_{i=j+1}^{k-1} \lambda_{ik} \omega_i$$

Now $v_j - w_j \in V_{j-1}$, so $\eta_j = 1$

$$\Rightarrow |\lambda_{jk} - \eta_j a_{jk}| = |\lambda_{jk} - a_{jk}| = |\mu_{jk}| \leq \frac{1}{2}$$

So the new coefficients for k are

$$\lambda'_{ik} := \begin{cases} \lambda_{ik} - a_{ik}\eta_i & \text{for } i \leq j \\ \lambda_{ik} & \text{for } i > j \end{cases}$$

and λ'_{jk} is weakly reduced.

$\rightarrow$ we can make all coeffs weakly reduced by applying this

- for all $1 \leq k \leq d$
  - and for fixed k for all $1 \leq j \leq k-1$ in decreasing order

$\rightarrow$ $\binom{d}{2}$ coeffs, in each round we touch at most d

$\Rightarrow$ can be done in $O(d^3)$.

Prop: We can make a lattice basis weakly reduced in $O(d^3)$ steps. ∎

$\rightarrow$ now turn this into a reduced basis:

The potential of $V = (v_1, \dots, v_d)$ is

$$D(V) := \prod_{j=1}^{d} \det \Lambda_j = \prod_{k=1}^{d} \prod_{j=1}^{k} \|w_j\|$$

Note: $D(V)$ depends on the order of the basis vectors!

Prop: $D(V) \geq \lambda_1^{\frac{d(d+1)}{2}} \prod_{j=1}^{d} \frac{1}{\sqrt{j}} \geq 1$

↑ first succ. min.