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

λ_1 = first succ. min.

proof u shortest vector in $\Lambda \setminus \{0\}$

$u_1, \dots, u_d$ — " — $\Lambda_d \setminus \{0\}$

$\Rightarrow \lambda_1 = \|u\| \leq \|u_d\|$

in a k-dim lattice Γ : $\min_{v \in \Gamma \setminus \{0\}} \|v\| \leq \sqrt{k}\,(\det \Gamma)^{1/k}$

$\Rightarrow \det \Lambda_j \geq \frac{\|u_j \cdots u^j\|}{\sqrt{\alpha_j}^j} \geq \frac{\lambda_1^j}{\sqrt{\alpha_j}^j}$ ∎

$\Rightarrow D(V)$ is bounded from below independent of the order of the basis

Assume $V = (v_1, \dots, v_d)$ weakly reduced and

$$\delta\, d(v_j, v_{j-1})^2 > d(v_{j+1}, v_{j-1})^2$$

Set $v_j' := v_{j+1}$, $v_{j+1}' := v_j$ and $v_k' := v_k$ for $k \neq j, j+1$

$\Rightarrow v_k' = v_k$ for $k \neq j, j+1$

$v_j' = \lim(v_1, \dots, v_{j-1}, v_{j+1})$, $v_{j+1} = \lim(v_1, \dots, v_j)$

$$\Rightarrow \quad \delta(v_j', v_{j-1})^2 \le d(v_{j+1}, v_{j-1})^2$$

But: $V' := (v_1', \dots, v_d')$ is not necessarily weakly reduced

$\rightarrow$ use above algorithm to make V' weakly reduced!

How many sweeps do we need?

Compute effect of a swap on $D(V)$

The new GS-Vectors are

$$w_i' = w_i \quad \text{for } i \neq j, j+1$$

$$w_j' := v_{j+1} - \sum_{i=0}^{j-1} \lambda_{i,j+1} w_i = v_{j+1} - \pi_{j-1}(v_{j+1})$$

$$w_{j+1}' := v_j - \sum_{i=1}^{j-1} \lambda_{i,j} w_i - \frac{\langle v_j, w_j' \rangle}{\|w_j'\|^2} w_j'$$

$$= v_j - \pi_{j-1}(v_j) - \frac{\langle v_j, w_j' \rangle}{\|w_j'\|} w_j'$$

Now by assumption

$$\frac{3}{4} d(v_j, v_{j-1}) > d(v_{j+1}, v_{j-1})^2$$

$$\Rightarrow \frac{3}{4} \|w_j\|^2 > \|w_j'\|^2 = \beta \|w_j\|^2 \quad \text{for some } \beta < \frac{3}{4}$$

As $\det \Lambda = \prod \|w_i\| = \prod \|w_i'\|$ and $w_i = w_i'$ for $i \neq j, j+1$

we get $\|w_{j+1}'\|^2 = \frac{1}{\beta} \|w_{j+1}\|^2$

$\Rightarrow \quad \det \Lambda'_i < \frac{\sqrt{3}}{2} \det \Lambda_i$

$\det \Lambda'_k = \det \Lambda_k \quad$ for $k \neq i$

$\Rightarrow D(v'_1, \dots, v'_d) < \frac{\sqrt{3}}{2} D(v_1, \dots, v_d)$

$\Rightarrow$ after at most $k = \left\lceil \frac{\log D}{\log \frac{2}{\sqrt{3}}} \right\rceil$ swaps the basis must be $\frac{3}{4}$-reduced.

As clearly $D \leq (\max \|v_i\|)^{\frac{d(d+1)}{2}}$

we need at most

$$k = \left\lceil \frac{1}{\log \frac{2}{\sqrt{3}}} \cdot \frac{d(d+1)}{2} \underbrace{\log \max \|v_i\|}_{\text{binary encoding lengths of input!}} \right\rceil$$

steps.

$\Rightarrow$ LLL needs at most $O(d^3 \cdot d^2(\log d + s))$

[missing: show that all intermediate values have encoding length at most poly(s)]

Note: There are improvements:

(1) Schnorr: $O(d^4(\log d + s))$

(2) Storjohann: $O(d^3(\log d + s))$

18. Integer Programming in Fixed Dimension

→ consist balls and ellipsoids.

Prop Λ lattice with basis $v_1, \dots, v_d$, $B = B_2$ unit ball with center z.
We can find in poly time
(1) either $u \in B \cap \Lambda$ or
(2) $c \in \Lambda^*$, $\|c\|_2 \le 2^{O(d^2)}$ s.th. $B \cap \Lambda$ is covered by at most $2^{O(d^2)}$ hyperplanes of the for $\langle c, x \rangle = \beta \in \mathbb{Z}$

proof: Assume $v_1, \dots, v_d$ is LLL-basis with orth. defect bounded by

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

Recall that $\|w_1\| \le \|w_2\| \le \dots \le \|w_d\|$

Case 1: $\|w_d\| \le \frac{1}{d}$ let $z = \sum \lambda_i v_i$, $u = \sum \lfloor \lambda_i \rfloor v_i \in \Lambda$

$$\Rightarrow \|u - z\| \le \sum \|v_i\| \le d \|w_d\| \le 1$$

$$\Rightarrow u \in B \cap \Lambda.$$

Case 2: $\|w_d\| > \frac{1}{d}$

Consider $H := \lim(v_1, \dots, v_{d-1})$

$$\rightarrow H + v_d = H + w_d \Rightarrow \Lambda \subseteq \bigcup_{\beta \in \mathbb{Z}} H + \beta v_d = \bigcup_{\beta \in \mathbb{Z}} H + \beta w_d$$

Now $\frac{\|v_d\|}{\|\omega_d\|} \le \tau \le \beta^{\frac{d(d-1)}{2}}$

$\Rightarrow \|\omega_d\| \ge \beta^{-\frac{d(d-1)}{2}} \quad \|v_d\| \ge \frac{1}{d}\beta^{-\frac{d(d-1)}{2}}$

Further: $\max_p (H+p v_d \cap B \neq \emptyset) - \min_p (H+p v_d \cap B \neq \emptyset) \le \beta$

$\Rightarrow H+p v_d \cap B \neq \emptyset$ for at most $\beta d \beta^{\frac{d(d-1)}{2}}$ p's

Let $c := \frac{\omega_d}{\|\omega_d\|^2}$.

Any $u \in \Lambda$ can be written as $u = \mu\omega_d + h$
$h \in H$, $\mu \in \mathbb{Z}$

$\Rightarrow \langle c, u\rangle = \mu \in \mathbb{Z} \Rightarrow c \in \Lambda^*$

and $\|c\| \le \frac{1}{\|\omega_d\|} \le \beta^{O(d^2)}$ ∎

Geometrically: Either a reduced basis has only short vectors or there is a short vector in the dual basis

Cor: The same holds for an ellipsoid $E = TB + a$

proof: Ex. Pull back to ball with T^{-1} and consider lattice $T^{-1}\Lambda$.

∎