Def A basis $v_1,\dots,v_n$ of $\mathbb{R}^n$ is LLL-reduced if its G-S basis and coeff. satisfy $|\mu_{ij}| \le \frac{1}{2}$ $\forall\, j<i$

Lenstra, Lenstra, Lovász
Arjen, Hendrik, László

and $\|v_{i+1}^*\|^2 \ge \frac{1}{2}\|v_i^*\|^2$.

Reference chapter 16 of "Modern Computer Algebra".

Lemma 13.5 Any $0 \neq r \in \Lambda$ satisfies

$$\|r\|^2 \ge \frac{1}{2^{n-1}} \cdot \|v_1\|^2 .$$

[v_1 is "almost" as short as possible.]

Pf Write $r = b_1 v_1 + \dots + b_k v_k$ with $k \le n$, $b_1,\dots,b_k \in \mathbb{Z}$, $b_k \neq 0$.

The component of r orthogonal to $\langle v_1,\dots,v_{k-1}\rangle$ is $b_k v_k^*$.

$$\Rightarrow \|r\| \ge \underbrace{|b_k|}_{\ge 1} \cdot \|v_k^*\| \ge \|v_k^*\| \ge \frac{1}{2^{k-1}} \cdot \|v_1^*\| = \frac{1}{2^{k-1}} \cdot \|v_1\| . \qquad \square$$

Thm 13.6 The following alg. computes an LLL-reduced basis of a lattice $\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$ (if it terminates).

Alg 13.6

1) Compute the G-S basis $v_1^*, \dots, v_n^*$ (which we'll keep up to date as we change $v_1, \dots, v_n$).

~~Start~~

~~Set~~ $i \leftarrow 1$.

While $i \le n$:

2) For $j = i-1, \dots, 1$:

Subtract round(μ_{ij}) times v_j from v_i to make $|\mu_{ij}| \le \frac{1}{2}$

$$\mu_{ij} = \frac{v_i \cdot v_j^*}{|v_j^*|^2}$$

3) If $i \ge 2$ and $|v_i^*|^2 < \frac{1}{2} |v_{i-1}^*|^2$:

4) Swap v_i, v_{i-1}. Recompute v_i^*, v_{i-1}^*.

Return to $i \leftarrow i-1$.

Otherwise:

Proceed to $i \leftarrow i+1$.

Return $v_1, \dots, v_n$.

Pf Correctness is clear: At the beginning of any while loop, $v_1, \dots, v_{i-1}$ satisfy the LLL-reducedness criterion. ∎

Rmk The alg. always terminates, but that's less obvious. We'll show that it has polynomial running time if $v_1, \dots, v_n \in \mathbb{Z}^n$.

Lemma 13.7 Let $v_1, \dots, v_n$ be a basis of $\mathbb{R}^n$ and $2 \le i \le n$ with $|\mu_{i,i-1}| \le \frac{1}{2}$ and $|v_i^*| < \frac{1}{2}|v_{i-1}^*|$.
Let $w_1, \dots, w_n$ be the same basis, but with v_i, v_{i-1} swapped.
Then:

a) $w_j^* = v_j^* \quad \forall j \ne i, i-1$. [$\Rightarrow$ We only need to update v_i^*, v_{i-1}^* in step 4.]

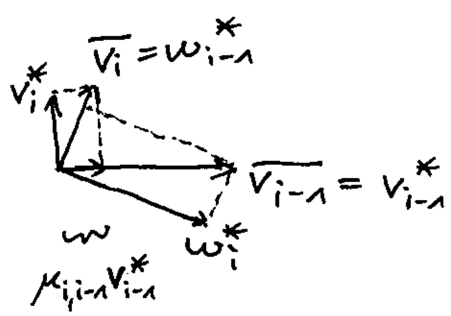
b) $|w_{i-1}^*|^2 < \frac{3}{4}|v_{i-1}^*|^2$ [$\Rightarrow$ Exponential decay.] [But $|v_{i-1}^*|^2 \in \mathbb{Q}$ might not be an integer!]

c) $|w_i^*| \le |v_{i-1}^*|$.

d) $|w_{i-1}^*| \cdot |w_i^*| = |v_{i-1}^*| \cdot |v_i^*|$.

Pf a) $\langle w_1, \dots, w_{j-1}\rangle = \langle v_1, \dots, v_{j-1}\rangle$ and $w_j = v_j$.

b–d) Only the components of v_{i-1}, v_i orthogonal to $\langle v_1, \dots, v_{i-2}\rangle$ matter for the computation of $v_{i-1}^*, v_i^*, w_{i-1}^*, w_i^*, \mu_{i,i-1}$.
Let $\overline{v_i}, \overline{v_{i-1}}$ be these components of v_i, v_{i-1}.



b) $|w_{i-1}^*|^2 = |v_i^*|^2 + \mu_{i,i-1}^2 |v_{i-1}^*|^2$ by Pythagoras

$$< \frac{1}{2}|v_{i-1}^*|^2 + \frac{1}{4}|v_{i-1}^*|^2 = \frac{3}{4}|v_{i-1}^*|^2.$$

c) clear

d) $|v_{i-1}^*|\cdot|v_i^*|$ = area of the parallelogram spanned by v_{i-1}, v_i

$|w_{i-1}^*|\cdot|w_i^*|$ = " " " w_{i-1}, w_i

$\square$

Rmk For any $0 \le k \le n$,

$$d_k := |v_1^*|^2 \cdots |v_k^*|^2$$

$$= \left(\begin{array}{l}k\text{-dimensional volume of the parallelepiped} \\ \text{spanned by } v_1, \dots, v_k\end{array}\right)^2$$

$$= \det(M_k),$$

for the $k \times k$-matrix $M_k = (v_i \cdot v_j)_{1 \le i,j \le k}$.

In particular, if $v_1, \dots, v_n \in \mathbb{Z}^n$, then $d_0, \dots, d_n \in \mathbb{Z}$.

Lemma 13.8 If $v_1, \dots, v_n$ lie in $\mathbb{Z}^n$ and $|v_1|, \dots, |v_n| \le B$, then Alg. 13.6 does at most $\mathcal{O}(n^2 \log B)$ swaps (line 4).

Pf Consider the integer $D = d_1 \cdots d_{n-1} > 0$.

In the beginning,

$$d_k = |v_1^*|^2 \cdots |v_k^*|^2 \le |v_1|^2 \cdots |v_k|^2 \le B^{2k},$$

so $D \le B^{2(1+\dots+(n-1))} = B^{n(n-1)}$

D only changes in line 4, in which it decreases at least by a factor of $\frac{4}{3}$.
(More precisely, d_{i-1} decreases, while $d_1, \dots, d_{i-2}, d_i, \dots, d_{n-1}$ remain the same.)
by Lemma 13.7 b

$\Rightarrow$ line 4 can only run $\mathcal{O}\left(\log_{\frac{4}{3}}\left(B^{n(n-1)}\right)\right) = \mathcal{O}(n^2 \log B)$ times

$\square$

Cor 13.9 Alg. 13.6 performs $\mathcal{O}(n^4 \log B)$ operations in $\mathbb{Q}$.

Pf 1) $\mathcal{O}(n^3)$

$$\mathcal{O}(n^2 \log B) \text{ times} \begin{cases} 2)\ \mathcal{O}(n^2) \\ 3)\ \mathcal{O}(n) \\ 4)\ \mathcal{O}(n^2) \end{cases}$$

$\square$

Lemma 13.10 For $v_1,\dots,v_n \in \mathbb{Z}^n$, we have

$$d_{k-1} v_k^* \in \mathbb{Z}^n.$$

Pf The orth. projection $v_k - v_k^*$ onto $\langle v_1,\dots,v_{k-1}\rangle$ is given by the formula

$$v_k - v_k^* = \underbrace{\begin{pmatrix} | & & | \\ v_1 & \cdots & v_{k-1} \\ | & & | \end{pmatrix}}_{\text{int. matrix}} \underbrace{M_{k-1}^{-1}}_{\frac{\text{int. mat.}}{\det(M_{k-1})}} \underbrace{\begin{pmatrix} — v_1 — \\ \vdots \\ — v_{k-1} — \end{pmatrix}}_{\text{int. matrix}} \underbrace{v_k}_{\in \mathbb{Z}^n}$$

$\square$

Cor 13.11 (bounds on denominators)

If $v_1,\dots,v_n \in \mathbb{Z}^n$ with $|v_1|,\dots,|v_n| \le B$, then in Alg. 13.6, the vectors v_k^* at any time satisfy $t v_k^* \in \mathbb{Z}^n$ for some $t \in \mathbb{Z}$ with $\log(t) = O(n \log B)$. ("bounded denominators")

Pf d_{k-1} is nonincreasing and $d_{k-1} = O(n \log B)$ in the beginning. $\square$

[How long can the vectors be?]

Lemma 13.12 If $|v_1|,\dots,|v_n| \le B$ in the beginning, then during Alg. 13.6:

a) $|v_1|,\dots,|v_n| \le \sqrt{n}\, B$

except possibly during step 2.

b) $|v_1|,\dots,|v_n| \le n\,(2B)^{2n}$

during step 2.

Cor 13.13 We always have $\log|v_1|,\dots,\log|v_n| \le O(n \log B)$ (for large B).
($\Rightarrow$ bound on numerators)

Pf a) holds in the beginning.

$\max(|v_1|,\dots,|v_n|)$ can only change during step 2 (where $|v_i|$ might change)

After step 2, $|\mu_{ij}| \le \frac{1}{2}$ $\forall j<i$.

Then, $|v_i|^2 = |v_i^*|^2 + \sum_{j<i} \mu_{ij}^2 |v_j^*|^2$.

By Lemma 13.7, $\max(|v_1^*|,\dots,|v_n^*|)$ is nonincreasing.

In the beginning, it's $\le B$.

$\Rightarrow |v_i|^2 \le B^2 + \sum_{j<i} \frac{1}{4} B^2 \le n B$.

b) At the beginning of step 2,

$$|\mu_{ij}| = \frac{|v_i \cdot v_j^*|}{|v_j^*|^2} \le \sqrt{n}\cdot B\cdot B\cdot B^{2(j-1)} = \sqrt{n}\cdot B^{2j} \le \sqrt{n}\cdot B^{2(n-1)}$$

because $|v_i| \le \sqrt{n}\cdot B$, $|v_j^*| \le B$, $|v_j^*|^2 = \frac{d_j}{d_{j-1}} \ge \frac{1}{d_{j-1}} \ge B^{-2(j-1)}$.

Moreover, $|v_j^*| \le |v_j| \le \sqrt{n} B$.

When subtracting $\mathrm{round}(\mu_{ij})\cdot v_j$ from v_i,

μ_{ik} changes by $|\mathrm{round}(\mu_{ij})\cdot \underbrace{\mu_{jk}}_{|\cdot| \le \frac{1}{2}}| \le \frac{1}{2}|\mu_{ij}| + \frac{1}{2}$

At the beginning of the for loop body in step 2 with index j, we have

$$\max(1, |\mu_{i,1}|, \dots, |\mu_{i,i-1}|) \leq 2^{i-j-1} \cdot \sqrt{n}\, B^{2(n-1)} \leq 2^{n-2} \cdot \sqrt{n} \cdot B^{2(n-1)}$$

(every time we handle an index j, the LHS at most increases by a factor of 2).

Then, $$|v_i|^2 = |v_i^*|^2 + \sum_{k<i} \mu_{ik}^2 |v_k^*|^2$$

$$\leq 2^{2(n-2)} n\, B^{4(n-1)} \cdot n B^2$$

$$\leq n^2 (2B)^{4n}.$$

□

Summary

Thm 13.13 If $v_1, \dots, v_n \in \mathbb{Z}^n$ with $|v_1|, \dots, |v_n| \leq B$, then Alg. 13.6 has running time $\tilde{O}(n^5 (\log B)^2)$ (on an $O(\log(n \log B))$-bit RAM).

Pf The rational numbers computed in the alg. have numerators and denominators with $O(n \log B)$ bits. This shows the claim with Cor 13.9.

□