Shortest vectors in 2 dimensions.

Gauss' Algorithm

$L \subseteq \mathbb{R}^2$

Want to find the shortest vector (ℓ_2)

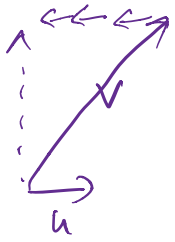
Start with a basis $\{u, v\}$ for L.

If needed, swap u, v so that $\|u\| \leq \|v\|$.

Keep doing the following:

- $m = \left\lceil \frac{\langle u, v \rangle}{\|u\|^2} \right\rfloor$

(Motivation: $v - \frac{\langle u, v \rangle}{\|u\|^2} \cdot u \perp u$)



- Replace v by $v - mu$

- If $\|v\| \geq \|u\|$, halt and output "u is shortest vector"

- Swap u, v

First: This algorithm terminates since $\|u\| + \|v\|$ strictly reduces at each iteration, and L is discrete.

Next Claim: When this algorithm terminates, we found the shortest vector.

Just before termination, the u, v that we have satisfy:

1. $\|v\| \geq \|u\|$
2. v is reduced by u.

   i.e. $|\langle v, u \rangle| \leq \frac{1}{2}$.

$\left| \frac{\langle u, v \rangle}{\|u\|^2} \right| \leq \frac{1}{2}$.

Want to show:

$$\|au + bv\| \geq \|u\|.$$

for all $(a,b) \in \mathbb{Z}^2$, $(a,b) \neq (0,0)$

$$\|au+bv\|^2 = a^2\|u\|^2 + b^2\|v\|^2 + 2ab\langle u,v\rangle$$

$$\geq \|u\|^2 \left(a^2 + b^2 - 2|ab| \cdot \frac{1}{2} \right)$$

AND. $a^2 + b^2 - |ab| \geq 1$

If $(a,b) \in \mathbb{Z}^2$ is nonzero.

so $\|au+bv\|^2 \geq \|u\|^2$

Analysis of Runtime [Assuming all entries of original basis are $\leq t$-bit integers]

we say we are making

good progress in a certain iteration if u and the new V satisfy

$$\|v\| < 0.9 \|u\|.$$

While we are making good progress $\|u\|$ keeps decreasing by a 0.9 factor in each iteration.

So $\leq O(t)$ iterations like this are possible.

Claim: If we don't make good progress in some iteration, then we halt within the next iteration.

Proof If we don't make good progress in some iteration, and haven't halted then our u and new V satisfy:

$$0.9\|u\| \leq \|v\| < \|u\|$$

- $\frac{|\langle v, u\rangle|}{\|u\|^2} \leq \frac{1}{2}$.

Want to show: in the next iteration we halt.

Let $\tilde{u} = v$
Let $\tilde{v} = u$ (swap).

Compute $\tilde{m} = \left\lceil \frac{\langle \tilde{v}, \tilde{u}\rangle}{\|\tilde{u}\|^2} \right\rfloor$

Set $new\text{-}\tilde{v} = \tilde{v} - \tilde{m}\tilde{u}$

Claim: $\|new\text{-}\tilde{v}\| \geq \|\tilde{u}\|$

$\tilde{m} = \left\lceil \frac{\langle \tilde{v}, \tilde{u}\rangle}{\|\tilde{u}\|^2} \right\rfloor = \left\lceil \frac{\langle u, v\rangle}{\|v\|^2} \right\rfloor$

$|\langle u, v\rangle| \leq \frac{1}{2}\|u\|^2 \leq 0.7\|v\|^2$

So $\tilde{m} \in \{-1, 0, 1\}$.

$$\text{new-}\tilde{v} \in \{\tilde{v}-\tilde{u},\ \tilde{v},\ \tilde{v}+\tilde{u}\}$$

$$= \{u-v,\ u,\ u+v\}.$$

Claim: true

$$\|u-v\|,\ \|u\|,\ \|u+v\| \geq \|v\|.$$

$$\|u-v\|^2 = \|u\|^2 + \|v\|^2 - 2\langle u,v\rangle$$

$$\geq \|v\|^2 + \|u\|^2 - 2\langle u,v\rangle$$

$$\geq \|v\|^2.$$

Similar for $\|u+v\|$.

LLL lattice basis reduction

Lenstra, Lenstra, Lovasz

Start with a lattice $L \subseteq \mathbb{R}^n$ (full rank) with a given basis $(b_1, \ldots, b_n)$.

Any other basis $(a_1, \ldots, a_n)$ looks like:

$$\begin{bmatrix} b_1 & \cdots & b_n \end{bmatrix} \begin{bmatrix} \ & \ & \ \\ \ & \ & \ \\ \ & \ & \ \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix}$$

$M \in GL_n(\mathbb{Z})$

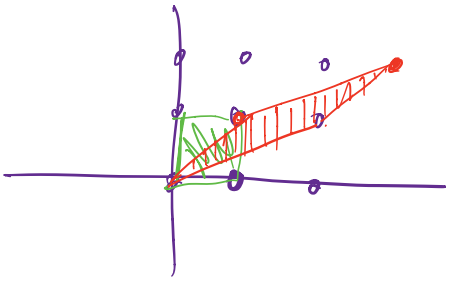
(integer matrix with integer inverse $\Leftrightarrow \det(M) = \pm 1$).

So:

$$\det(b_1, \dots b_n) = \det(a_1, \dots a_n) \boxed{= \det(L)}$$

$$\| \text{Vol}\left(\text{parallelopiped } \sum_{i=1}^{n} t_i b_i, \ t_i \in [0,1]\right)$$

Such parallelopipeds tile $\mathbb{R}^n$ when shifted by L, are called fundamental parallelopipeds for L.



Observation (Hadamard's inequality) $\det(L) \leq \prod \|b_i\|$

$\| \det(b_1, \dots b_n)$ for any basis

$(b_1, \ldots b_n)$.

Equality iff b_i's are orthogonal.

Orthogonality defect of a basis

$$OD(b_1, \ldots b_n) = \frac{\prod \|b_i\|}{\det(L)}$$

Thm Every lattice has a basis $(b_1 \ldots b_n)$ with $OD(b_1, \ldots b_n) \leq n^{O(n)}$.

LLL will find a basis with orthogonality defect $\leq 2^{O(n^2)}$.

in $\text{poly}(n, t)$ time where all entries of our starting basis for L are $\leq t$-bit integers.