LLL lattice reduction

$L \subseteq \mathbb{R}^n$ full rank lattice.

$(b_1, \ldots b_n)$ ordered basis for L.

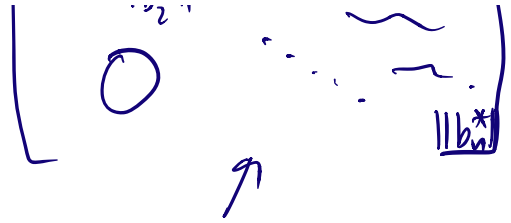
Associated to $b_1, \ldots b_n$ is

unit vectors $u_1, \ldots u_n$, orthonormal s.t. $[b_1, b_2 \cdots, b_n]$ when viewed in this coordinate system, is upper triangular.

$b_i^* =$ b_i − projection (b_i) onto span $(b_1, \ldots b_{i-1})$

$u_i = \dfrac{b_i^*}{\|b_i^*\|}$.

$A(b_1 \ldots b_n) =$ $\begin{bmatrix} \|b_1^*\| & & & A_{ij} \\ & \|b_2^*\| & & \\ & & \ddots & \\ & & & \|b_n^*\| \end{bmatrix}$



column i is b_i written in coordinates $(u_1, \dots u_n)$

Weakly reduced: $|A_{ij}| \leq \frac{\|b_i^*\|}{2}$. $\forall i<j$

LLL-reduced: Weakly reduced and

for each i, Let λ, λ' be the projections of b_i, b_{i+1} on span of u_i, u_{i+1}.

Want $\|\lambda''\| \geq 0.9\|\lambda\|$ (*)

[Consider lattice L^* generated by λ, λ'

in $\mathbb{R}^2 \simeq \text{span}(u_i, u_{i+1})$,

then (λ, λ') being weakly reduced

and $\|\lambda'\| \geq \|\lambda\| \iff \lambda$ is shortest

vector in L^*]

Thm Can find LLL reduced bases in $\text{poly}(n,t)$ time. (where all entries of the given basis of the lattice are t-bit integers).

Thm If $(b_1, \ldots b_n)$ is LLL-reduced then $\|b_1\| \leq 2^{O(n)}$. shortest vector in L.

Thm If $(b_1, \ldots, b_n)$ is LLL-reduced then $OD(b_1, \ldots, b_n) \leq 2^{O(n^2)}$.

Thm Given a basis of L with $OD(b_1, \dots b_n) \leq C$, we can find a shortest vector in time $\text{poly}(n, t, C^n)$.

LLL algorithm

Start with initial bases $(b_1, \dots b_n)$

While not LLL reduced, do:

Make $(b_1, \dots b_n)$ weakly reduced

If For some i, b_i, b_{i+1} violate (*)

swap b_i, b_{i+1}.

Done

Analysis

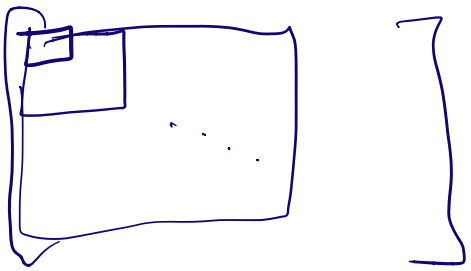
If algorithm stops, the result is

LLL-reduced.

Define potential function. $\Phi(b_1, \cdots, b_n)$

as follows:

Take $A(b_1, \cdots b_n)$



$$\Phi(b_1, \cdots b_n) = \prod_{j=1}^{n} \det\left(A^{(b_1, \cdots b_n)}_{[i]\times[i]} \right)$$

$$= \prod_{j=1}^{n} \prod_{\ell=1}^{j} \|b_\ell^*\|$$

$$= \prod_{i=1}^{n} \|b_i^*\|^{n-i+1}$$

Claim: Weak reduction does not change Φ.

(Weak reduction does not change $u_1, \ldots u_n$ and the diagonal of A).

Claim If b_i, b_{i+1} violate (*), then swapping b_i, b_{i+1} reduces Φ by a constant factor.

Proof If we swap b_i, b_{i+1}, then $b_1^*, b_2^*, \ldots b_{i-1}^*, b_{i+2}^*, \ldots b_n^*$ are unchanged.

Only b_i^*, b_{i+1}^* change.

Condition (*) violated

$$\begin{bmatrix} \|b_i^*\| & A_{i,i+1} \\ & \|b_{i+1}^*\| \end{bmatrix}$$

$$\Downarrow$$

$$\|b_{i+1}^*\|^2 + \left(A_{i,i+1}\right)^2 < 0.9 \cdot \|b_i^*\|^2$$

After swap:

$\leftarrow \begin{pmatrix} A_{i,i+1} \\ \|b_{i+1}^*\| \end{pmatrix}$ is first vector,

$\begin{pmatrix} \|b_i^*\| \\ 0 \end{pmatrix}$ is the second vector.

The new $\|b_i^*\|$ equals the length of $\begin{pmatrix} A_{i,i+1} \\ \|b_{i+1}^*\| \end{pmatrix} < 0.9 \|b_i^*\|$ old.

The new $\|b_{i+1}^*\| = \dfrac{\text{Old } \|b_i^*\| \cdot \text{Old } \|b_{i+1}^*\|}{\text{New } \|b_i^*\|}$.

New $\|b_i^*\| < 0.9 \cdot$ old $\|b_i^*\|$

New $\|b_{i+1}^*\|$ · New $\|b_i^*\|$ = Old $\|b_{i+1}^*\|$ · Old $\|b_i^*\|$

$\Rightarrow$ Φ $(b_1, \ldots b_n)$ reduced by a factor 0.9

Φ starts off $\leq 2^{\text{poly}(n,t)}$.

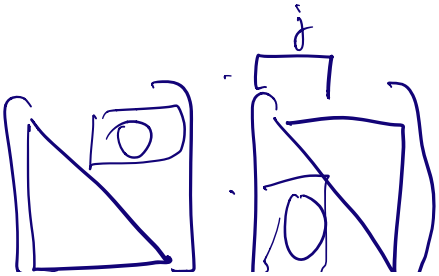
Φ is always $\lceil$ integer $\rceil$

So $\Phi \geq 1$.

$$\begin{bmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{bmatrix} = \begin{bmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{bmatrix} \begin{bmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{bmatrix}$$

B $\qquad$ U $\qquad$ A

$B^T B = A^T A$.



Upper left $j \times j$ submatrix of $A^T A$

$=$ (upper left $j \times j$ submatrix of A^T)

$\times$ (upper left $j \times j$ matrix of A)

(since A is upper triangular)

$$= \det\left(A_{[j]\times[j]}\right)^2$$

$$\Phi(b_1, \ldots b_n)^2 = \prod_{j=1}^{n} \det\left((B^T B)_{[j]\times[j]}\right)$$

$$\in \mathbb{Z}.$$

[Did not prove: all intermediate integers are $\leq$ poly(n,t) bits long].

Proof that LL-reduced bases are nice.

Condition (*)

$$\Rightarrow \|b_{i+1}^*\|^2 + |A_{i,i+1}|^2 \geq 0.9 \cdot \|b_i^*\|^2$$

Weak-reducedness

$$\Rightarrow \quad |A_{i,i+1}| \leq \frac{\|b_i^*\|}{2}.$$

So $$0.9\,\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2 + \frac{\|b_i^*\|^2}{4}$$

$$\Rightarrow \|b_i^*\|^2 \leq \frac{\|b_{i+1}^*\|^2}{0.9 - 0.25}$$

$$\leq 2\,\|b_{i+1}^*\|^2.$$

So $\|b_i^*\|$'s are not decreasing too rapidly as i increases

$$\|\text{Shortest vector}\| \geq \min_i \|b_i^*\|$$

$$\geq 2^{-n/2} \cdot \|b_1^*\|$$

$$= 2^{-n/2} \|b_1\|.$$

So b_1 is an approximate shortest vector.

Analysis of OD.

Want to say: $\dfrac{\prod \|b_i\|}{\prod \|b_i^*\|} \leq 2^{O(n^2)}$.

$$\|b_i\|^2 = \left(\sum_{l<i} |A_{li}|^2\right) + \|b_i^*\|^2.$$

$$\begin{bmatrix} & & i & \\ & & \vdots & \\ & & \|b_i^*\| & \\ & & 0 & \\ & & \vdots & \\ & & 0 & \end{bmatrix}$$

$$\leq \sum_{l<i} \frac{\|b_l^*\|^2}{4} + \|b_i^*\|^2$$

$$\leq \left(\sum_{l<i} \frac{\|b_i^*\|^2 \cdot 2^{i-l}}{4} \right) + \|b_i^*\|^2.$$

$$\leq 2^n \cdot \|b_i^*\|^2.$$

So done.

Finding exact shortest vectors.

Given $\begin{bmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{bmatrix}$, want to

minimize $\|\sum x_i b_i\|$ as $(x_1, \ldots x_n)$ vary in $\mathbb{Z}^n$.

Let v be the shortest vector in L.

Solution x to

$$\begin{bmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{bmatrix} \begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} v \end{pmatrix}$$

is given by Cramer's rule,

$$x_i = \frac{\det\left(b_1, \ldots b_{i-1}, v, b_{i+1}, \ldots b_n \right)}{\det\left(b_1, \ldots b_n \right)}$$

$$\leq \frac{\prod_{\substack{j=1 \\ j \neq i}}^{n} \|b_j\| \cdot \|v\|}{\det\left(b_1, \ldots b_n \right)}$$

$$\leq \underbrace{\prod_i \|b_i\|}_{\det(b_1,\ldots b_n)} \leq OD(b_1,\ldots b_n)$$

Algorithm try all

$$(x_1,\ldots x_n) \in [-OD, OD]^n$$

and output $\sum x_i b_i$

with smallest norm.

So in time $poly(2^{poly(n)}, t)$,

we can find exact shortest vectors in Lattices.