Finding short vectors in lattices

LLL algorithm

Thm Given a lattice L in $\mathbb{R}^n$, specified by a basis all coordinates of which are $\leq t$-bit integers.

we can find in time $\text{poly}(n, t)$

1. a vector $v \in L$ s.t.

$$\|v\| \leq \underbrace{2^{O(n)}}_{} \cdot \min_{u \in L \setminus \{0\}} \|u\|$$

2. a basis $b_1, \ldots, b_n$ of L s.t.

$$OD(b_1, \ldots, b_n) := \frac{\prod_i \|b_i\|}{\det([b_1, \ldots, b_n])}$$

$$\leq 2^{O(n^2)}.$$

How to give a lower bound on the length of the shortest vector in a lattice.

Start with any basis $b_1, \dots b_n$.

We will look at the Gram-Schmidt orthonormal basis associated to $b_1, \dots b_n$.

$$b_1^* = b_1$$

$$u_1 = \frac{b_1^*}{\|b_1^*\|}$$

b_2^* = component of b_2 orthogonal to b_1

$$u_2 = \frac{b_2^*}{\|b_2^*\|}$$

b_3^* = component of b_3 orthogonal

to $\text{span}(b_1, b_2)$
$= \text{span}(b_1^*, b_2^*)$

$$u_3 = \frac{b_3^*}{\|b_3^*\|}$$

$\vdots$

b_i^* = component of b_i orthogonal to $\text{span}(b_1, \dots b_{i-1})$

$$= b_i - \sum_{j=1}^{i-1} \langle b_i, u_j \rangle \cdot u_j$$

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

$\vdots$

Write $b_i = \sum A_{ji} u_j$

The u_i's are an orthonormal basis, so $\|b_i\|^2 = \sum_j A_{ji}^2$

In this u_i coordinate system on $\mathbb{R}^n$, the $[b_1 \dots b_n]$

matrix looks like:

$$A(b_1, \dots b_n) = \begin{bmatrix} \|b_1^*\| & u & \cdots & \\ 0 & \|b_2^*\| & \cdots & \\ 0 & 0 & \ddots & \\ \vdots & \vdots & \|b_i^*\| & \\ 0 & 0 & 0 & \|b_n^*\| \end{bmatrix}$$

i^{th} entry of the column i is the coefficients of u_j in

$$b_i = \sum A_{ji} u_j$$

For 2x2, if we have u, v basis for L, then the corresponding matrix looks like

$$\begin{bmatrix} \|u\| & \frac{\langle v, u \rangle}{\|u\|} \\ 0 & \left\| v - \frac{\langle v, u \rangle}{\|u\|} \frac{u}{\|u\|} \right\| \end{bmatrix}$$

Defn $b_1, \ldots b_n$ is called weakly reduced if in the above matrix $A(b_1, \ldots b_n)$ every entry of row i has absolute value at most $\frac{|A_{ii}|}{2}$.

Thm Any basis $(b_1, \ldots b_n)$ can be made weakly reduced with $O(n^2)$ operations of the form

$$b_j = b_j + m\, b_i$$

for $i < j$.

Proof Key point.

Operations $b_j = b_j + m \cdot b_i$ for $i < j$ don't change the orthonormal basis $u_1, \ldots u_n$ of $\mathbb{R}^n$.

So these operations affect $A(b_1, \dots b_n)$ by the corresponding simple column operations.

Then fix the ij entry for $j > i$ using

$$b_j = b_j + m \cdot b_i \qquad m = -\left\lceil \frac{A_{ij}}{\|b_i^*\|} \right\rfloor$$

first for $i = n$, then $i = n-1$, then $i = n-2$, ... , finally $i = 1$.

Is weakly reduced enough to get a pretty short vector?

NO. In 2-d this just the Gauss algorithm without swapping,

$$\begin{bmatrix} F_n & F_{n-2} \\ F_{n+1} & F_{n-3} \end{bmatrix}$$

$$\frac{|\langle u, v \rangle|}{\|u\|^2} < \frac{1}{2} \; ?$$

Lemma

Given a basis $(b_1, \ldots b_n)$ for L, every nonzero vector in L has length $\geq \min_i \|b_i^*\|$

Why?

$$\left\| \sum_i \alpha_i b_i \right\|^2 \qquad \alpha_i \in \mathbb{Z}$$

$$= \left\| \sum_i \alpha_i \left(\sum_{j \leq i} A_{ji} u_j \right) \right\|^2$$

$$= \left\| \sum_{i,j} \alpha_i A_{ji} u_j \right\|^2$$

$$= \sum_j \left(\sum_{i \geq j} \alpha_i A_{ji} \right)^2$$

If k is the largest k s.t.

$\alpha_k \neq 0$, then $\left| \sum_{i \geq k} \alpha_i A_{ki} \right|$

$= |\alpha_k A_{kk}|$

$\geq 1 \cdot \|b_k^*\|$

So $\| \sum \alpha_i b_i \| \geq \|b_k^*\|$

Goal: Find a basis so that the $\min_k \|b_k^*\|$ is as large as possible.

A basis $(b_1, \cdots b_n)$ is called LLL reduced if

(1). It is weakly reduced

(2) Consider the projections λ, λ' of b_i and b_{i+1} onto

the span $\{u_i, u_{i+1}\}$

Want $\|\lambda'\| \geq 0.9 \|\lambda\|$

$\lambda = A_{ii}\, u_i$

$\lambda' = A_{i,i+1}\, u_i + A_{i+1,i+1}\, u_{i+1}$

Want: $A_{i,i+1}^2 + A_{i+1,i+1}^2 \geq (0.9)^2 \|A_{ii}\|^2$

Without 0.9, this is the statement that λ is the smallest vector in the 2d lattice $\mathbb{Z}$-spanned by λ, λ'. [Because of the Gauss algorithm]