Lattices

A lattice in $\mathbb{R}^n$ is a discrete subgroup under addition

Thm For every lattice L in $\mathbb{R}^n$, there are $m \leq n$ vectors $v_1, \ldots, v_m$ s.t.

$$L = \left\{ \sum a_i v_i \;:\; a_i \in \mathbb{Z} \right\}$$

$\Leftarrow$

$L = \mathbb{Z}^n \subseteq \mathbb{R}^n$

$L = M \cdot \mathbb{Z}^n$ where M is an invertible $n \times n$ matrix in $\mathbb{R}^n$.

- $\left\{ (a + b\sqrt{2}, 0) \;;\; a, b \in \mathbb{Z} \right\} \subseteq \mathbb{R}^2$ is not a lattice.

$$\begin{pmatrix} 1 & \sqrt{2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Thm $\Rightarrow$ All lattices are of the form

($M \cdot \mathbb{Z}^m \subseteq \mathbb{R}^n$.

where M is a $n \times m$ rank m matrix, (for $m \leq n$).)

$e_i = (0 \cdots 0, \underset{i}{1}, 0 \cdots 0)$

e_1, e_2 generate $\mathbb{Z}^2 \subseteq \mathbb{R}^2$

$e_1, e_1 + e_2$ .... $\mathbb{Z}^2 \subseteq \mathbb{R}^2$.

$7e_1 + 5e_2$, $10e_1 + 7e_2$ ... $\mathbb{Z}^2 \subseteq \mathbb{R}^2$.

Basic algorithmic questions about lattices.

1. SVP - shortest vector problem

   Given a lattice L, what is the $w \in L$ s.t. $w \neq 0$ and $\|w\|$ is minimized?

2. CVP - closest vector problem.

Given a lattice $L \subseteq \mathbb{R}^n$, $x \in \mathbb{R}^n$,

find $w \in L$ that minimizes $\|w - x\|$.

Assume the lattice is specified with a basis $b_1, \ldots, b_m \in \mathbb{Z}^n$

(this is with loss of generality, but algorithmically is as interesting).

Assume that all entries of b_i are $\leq t$-bit integers.

So input has size: tmn bits.

Ideally, would like to solve this in time $\text{poly}(t, m, n) = \text{poly}(t, m)$

We know:

1. If $P \neq NP$, CVP, SVP don't have poly(t, n) time algorithms.

2. There is a $2^{\text{poly}(n)} \cdot \text{poly}(t)$ algorithm for CVP, SVP. $\Rightarrow$

3. There is a poly(n, t) time algorithm to find $2^{O(n)}$-approximate shortest vectors / closest vectors. (LLL)

Proof of structure thm for lattices

Let L be a lattice.

Step 1 L is finitely generated.

Take $v_1, \ldots v_m \in L$ s.t. $\mathbb{R}\text{-span}(v_1, \ldots v_m)$

contains L, and $v_1, \dots v_m$ are $\mathbb{R}$-linearly independent.

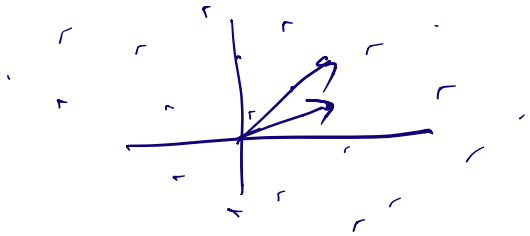
$$K = \left\{ \sum_{i=1}^{m} a_i v_i \;:\; a_i \in \mathbb{Z} \right\} \subseteq \underbrace{\text{"}\mathbb{R}^m\text{"}}_{\text{"}\mathbb{R}\text{-span}(L)\text{"}}$$

$K \subseteq L$. K is a lattice.

If L not finitely generated, we can take vectors $v_{m+1}, v_{m+2}, \dots$

where $v_i \notin \mathbb{Z}\text{-span}\{v_1, \dots v_{i-1}\}$.

Claim $\exists B$ s.t. Every $u \in \mathbb{R}\text{-span}(L)$ is within distance B of some element of K.



Proof $u = \sum \alpha_i v_i$ for some $\alpha_i \in \mathbb{R}$

Consider $w = \sum_{i=1}^{m} \lfloor \alpha_i \rceil v_i \in K$.

So $w - u = \sum_i (\alpha_i - \lfloor \alpha_i \rceil) v_i$

$$\|w-u\| \leq \sum_i \|v_i\|$$

For each $i>m$, $\exists\ w_i \in K$ s.t.

$$0 < \|v_i - w_i\| \leq B.$$

The $v_i - w_i$ are all distinct.

And the $v_i - w_i$ are all in L.

Contradiction to discreteness.

---

so L is finitely generated.

Step 2:

$$\mathbb{Q}\text{-span}\{v_1, \dots, v_m\} \supseteq L.$$

Take any $w \in L$.

Write $w = \sum_{i=1}^{m} \alpha_i v_i$, $\alpha_i \in \mathbb{R}$.

If α_i are not all rational,

let us find $h \in \mathbb{Z}$ s.t. each

$h\alpha_i \in \mathbb{R}$ is within distance $\leq \epsilon$ from $\mathbb{Z}$.

[Proof: Take $H = 2\left(\frac{1}{\epsilon}\right)^m$. Consider

$(\alpha_1, \dots \alpha_m) \bmod 1$

$(2\alpha_1, \dots 2\alpha_m) \bmod 1$

$\vdots$

$(H\alpha_1, \dots, H\alpha_m) \bmod 1$

$\in [0,1)^m$

Some two of these H pts must be ϵ-close.

Their difference has the desired property.]

So $hw = \sum_{i=1}^{m} h\alpha_i v_i \in L$

$= \sum \lceil h\alpha_i \rceil v_i + \sum \left(h\alpha_i - \lceil h\alpha_i \rceil\right) v_i$

$\lfloor \beta \rceil$ = nearest integer to β.

$\in L$ $\qquad$ $\leq \epsilon \left(\sum \|v_i\|\right)$

So $\left(hw - \sum_i \lfloor h\alpha_i \rceil v_i\right) \in L \setminus \{0\}$.

and has norm $\leq O(\epsilon)$.

This holds for all $\epsilon > 0$, so contradicts discreteness.

Step 3

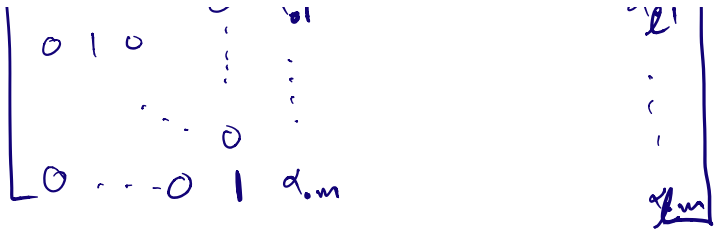
Take $v_1, \ldots v_m, v_{m+1}, \ldots, v_\ell$ that generate L.

We know that each $v_j \in \mathbb{Q}$-span of $v_1, \ldots v_m$.

Write each $v_j = \sum_{i=1}^{m} q_{ji} v_i$

$\downarrow$ $\qquad$ $\downarrow$ $\downarrow$

$\lceil 100 \cdots \alpha_{\cdot} \qquad \alpha_{\cdot \cdot} \rceil$



All the α_{ji} are rational.

$\mathbb{Z}$-span of the columns is L in the basis v_i.

Take out common denominators.

and Hermite Normal Form tells us that

finitely generated

any subgroup of $\mathbb{Q}^m$ is $\mathbb{Z}$-generated by $\leq m$ vectors.

$$L = \mathbb{Z}\text{col span of} \rightarrow \begin{bmatrix} \frac{1}{2} & \frac{1}{3} & 1 \\ 2 & 1/2 & 2 \end{bmatrix}$$

$$\begin{matrix} \frac{1}{6} \cdot \\ \frac{1}{2} \cdot \end{matrix} \begin{bmatrix} 3 & 2 & 6 \\ 4 & 1 & 4 \end{bmatrix}$$

$\downarrow$ HNF

$$\begin{matrix} \frac{1}{6} \\ \frac{1}{2} \end{matrix} \begin{bmatrix} a & 0 & 0 \\ b & c & 0 \end{bmatrix}$$

$$\begin{bmatrix} \frac{a}{6} & 0 & 0 \\ \frac{b}{2} & \frac{c}{2} & 0 \end{bmatrix}$$ & column span equalls L
