Lattice and breaking knapsack

Collision

$M = (M_1, \ldots, M_n)$

S

want x_i s.t.

$\sum x_i M_i = S$

$x_i \in \{0, 1\}$

Brute force: test every subset

$O(2^n)$

Collision

for $I \subseteq \{i \mid 1 \le i \le n/2\}$

compute $A_I = \sum_{i \in I} M_i$

$J \subseteq \{j \mid n/2 < j \le n\}$

compute $B_J = S - \sum_{j \in J} M_j$

Look for matches

If $A_I = B_J$, then

$\sum_{i \in I} M_i = S - \sum_{j \in J} M_j$

$S = \sum_{i \in I} M_i + \sum_{j \in J} M_j$

$M = \{5, 9, 15, 23, 28, 35\}$

$S = 78$

$\{I\} = 2^{\{1,2,3\}}$

$\{A_I\} = \{0, 5, 9, 15, 14, 20, 24, 29\}$

$\{J\} = 2^{\{4,5,6\}}$

$\{B_J\} = \{78, 55, 50, 43, 27, 29, 15, -8\}$

If $I = \{2, 3\}$

then $A_I = M_2 + M_3 = 24$.

15: $78 = 15 + 28 + 35$

20: $78 = 5 + 15 + 23 + 35$

$O(2^{n/2+\varepsilon})$

Lattice

Dfn: $\vec{v}_1, \dots, \vec{v}_n \in \mathbb{R}^n$ LI

the lattice generated by $\{\vec{v}_1, \dots, \vec{v}_n\}$ is

$$L = \{a_1\vec{v}_1 + \cdots + a_n\vec{v}_n \mid a_i \in \mathbb{Z}\}$$

An Integral lattice is a lattice w/ $\vec{v}_i \in \mathbb{Z}^n$.

$\mathbb{Z}^\times = \{1, -1\}$

$n = 3$

$$\vec{v}_1 = \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix}, \vec{v}_2 = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}, \vec{v}_3 = \begin{bmatrix} 2 \\ -3 \\ -5 \end{bmatrix}$$

$$\vec{w}_1 = \vec{v}_1 + \vec{v}_3 = \begin{bmatrix} 4 \\ -2 \\ -2 \end{bmatrix}$$

$$\vec{w}_2 = \vec{v}_1 - \vec{v}_2 + 2\vec{v}_3 = \begin{bmatrix} 5 \\ -7 \\ -7 \end{bmatrix}$$

$$\vec{w}_3 = \vec{v}_1 + 2\vec{v}_2 = \begin{bmatrix} 4 \\ 5 \\ 3 \end{bmatrix}$$

$$U = \begin{bmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$

$$\det(U) = 0 + 0 + 2 - (-1 + 4 + 0) = -1.$$

need U invertible over $\mathbb{Z}$

and $-1 \in \mathbb{Z}^\times$ is invertible.

So $\vec{w}_1, \vec{w}_2, \vec{w}_3$ is a basis for L

$$U^{-1} = \begin{bmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{bmatrix}$$

$$\vec{v}_1 = 4\vec{w}_1 - 2\vec{w}_2 - \vec{w}_3$$

$$\vec{v}_2 = -2\vec{w}_1 + \vec{w}_2 + \vec{w}_3$$

$$\vec{v}_3 = -3\vec{w}_1 + 2\vec{w}_2 + \vec{w}_3$$

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{bmatrix} = \begin{bmatrix} \vec{v}_1^T \\ \vec{v}_2^T \\ \vec{v}_3^T \end{bmatrix}$$

then

$$B = UA = \begin{bmatrix} 4 & -2 & -2 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{bmatrix} = \begin{bmatrix} \vec{w}_1^T \\ \vec{w}_2^T \\ \vec{w}_3^T \end{bmatrix}$$

Let $L \subseteq \mathbb{R}^3$ generated by $\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}$

$L_2 \subseteq \mathbb{R}^3$ gen by $\begin{bmatrix}2\\0\\0\end{bmatrix}, \begin{bmatrix}0\\3\\0\end{bmatrix}, \begin{bmatrix}0\\0\\4\end{bmatrix}$

$$U = \begin{bmatrix}2&0&0\\0&3&0\\0&0&4\end{bmatrix} \qquad U^{-1} = \begin{bmatrix}1/2&0&0\\0&1/3&0\\0&0&1/4\end{bmatrix}$$

$\det(U) = 24$

not invertible on $\mathbb{Z}$

$(24 \in \mathbb{Z}^\times)$

Defn: $L \subseteq \mathbb{R}^n$

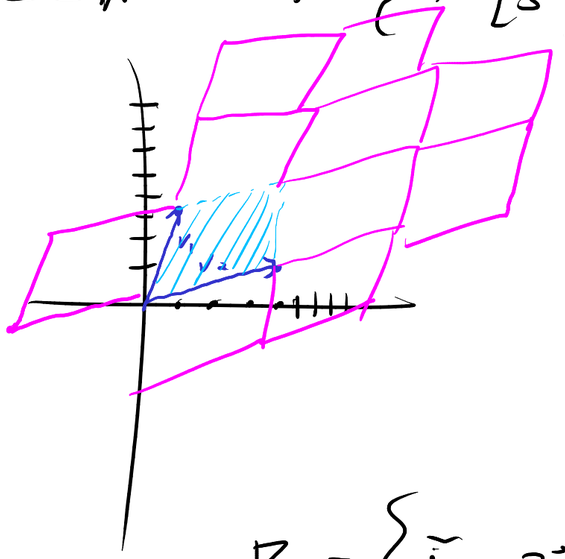
$B = \{\vec{v}_1, \dots, \vec{v}_n\}$

Then the fundamental domain for L corresponding to B is

$$\mathcal{F}(B) = \{t_1\vec{v}_1 + t_2\vec{v}_2 + \cdots + t_n\vec{v}_n \mid 0 \le t_i < 1\}$$

Fact: every $\vec{w} \in \mathbb{R}^n$ can be written uniquely as $\vec{w} = \vec{t} + \vec{v}$ for some $\vec{t} \in \mathcal{F}$, $\vec{v} \in L$.

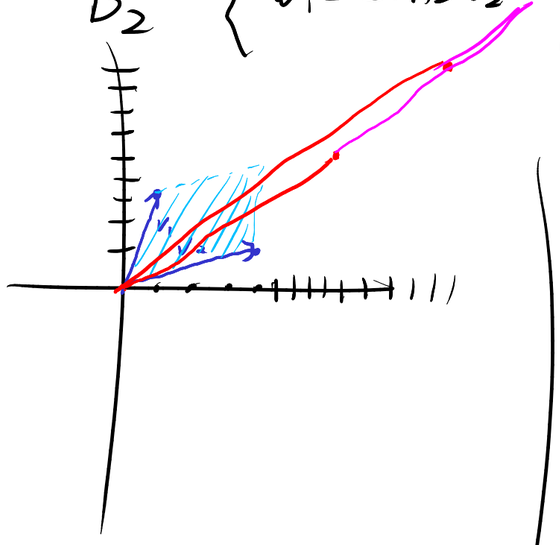
$L \subseteq \mathbb{R}^2$ $\quad B_1 = \left\{\vec{v}_1 = \begin{bmatrix}1\\3\end{bmatrix}, \vec{v}_2 = \begin{bmatrix}4\\1\end{bmatrix}\right\}$



$$U = \begin{bmatrix}2 & 3\\ 1 & 2\end{bmatrix} \quad \det U = 1$$

$$U^{-1} = \begin{bmatrix}2 & -1\\ -3 & 2\end{bmatrix}$$

$B_2 = \left\{\vec{w}_1 = 2\vec{v}_1 + 3\vec{v}_2 = \begin{bmatrix}14\\9\end{bmatrix}, \vec{w}_2 = \vec{v}_1 + 2\vec{v}_2 = \begin{bmatrix}9\\5\end{bmatrix}\right\}$



$$\det A = \det\begin{bmatrix}1 & 3\\ 4 & 1\end{bmatrix} = -11$$

$$\det B = \det\begin{bmatrix}14 & 9\\ 9 & 5\end{bmatrix} = 70 - 81 = 11.$$

Def: $L \subseteq \mathbb{R}^n$

$\mathcal{F}$ FD

then the n-dim volume of $\mathcal{F}$ is the

<u>covolume</u> or <u>determinant</u> of L, $\det(L)$

Fact: $L \subset \mathbb{R}^n$

$B = \{\vec{v}_1, \dots, \vec{v}_n\}$ basis of L,

$\mathcal{F}(B)$ FD

If $A = \begin{bmatrix} \vec{v}_1^T \\ \vec{v}_2^T \\ \vdots \\ \vec{v}_n^T \end{bmatrix}$,

then $|\det(A)| = \det L$.

Further,

$\det L \le \|\vec{v}_1\| \cdot \dots \cdot \|\vec{v}_n\|$

Cor: if $B_1 = \{\vec{v}_i\}$

$B_2 = \{\vec{w}_i\}$

2 bases for L,

$A = \begin{bmatrix} \vec{v}_1^T \\ \vdots \\ \vec{v}_n^T \end{bmatrix}$ $B = \begin{bmatrix} \vec{w}_1^T \\ \vdots \\ \vec{w}_n^T \end{bmatrix}$

then $|\det A| = |\det B|$

Pf: $A = UB$

$\det A = \det(UB)$

$= \det(U)\det(B)$

$= \pm \det(B)$.

$L = \mathbb{R}^2$

$\mathbb{Z}^2$ [i] gen by $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Shortest Vector Problem

Given lattice L
basis B

find a shortest $\vec{v} \in L$.

NP-complete.

Closest-vector problem:

Lattice L, basis B,
$\vec{w} \in \mathbb{R}^n$

find $\vec{v} \in L$ closest to $\vec{w}$.

Lenstra–Lenstra–Lovasz algorithm
can solve this approximately
in poly time.

Find a vector at most $2^{n-1/2}$ times
length of shortest vector

Hermite's Thm
L contains a $\vec{v} \neq \vec{0}$ s.t.

$$\|\vec{v}\| \leq \sqrt{n} \det(L)^{1/n}$$

Gaussian Heuristic
expected shortest length is

$$\sigma(L) = \sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}.$$

want to solve SS problem

for $M = (M_1, \dots, M_n)$

S

$$\begin{bmatrix} 2 & 0 & 0 & \cdots & 0 & M_1 \\ 0 & 2 & 0 & \cdots & 0 & M_2 \\ 0 & 0 & 2 & \cdots & 0 & M_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2 & M_n \\ 1 & 1 & 1 & \cdots & 1 & S \end{bmatrix} = \begin{bmatrix} \vec{v}_1^{\,T} \\ \vec{v}_2^{\,T} \\ \vdots \\ \vec{v}_n^{\,T} \\ \vec{v}_{n+1}^{\,T} \end{bmatrix}$$

lattice $L \subseteq \mathbb{R}^{n+1}$ generated by $\{\vec{v}_i\}$

Suppose $\vec{x} = (x_1, \dots, x_n)$ is a soln.

Then $\vec{t} = \left(\sum_{i=1}^{n} x_i \vec{v}_i\right) - \vec{v}_{n+1}$

$= (2x_1 - 1, 2x_2 - 1, \dots, 2x_n - 1, 0) \in L$

$\|\vec{t}\| = \sqrt{n}$

$\sigma(L) = \sqrt{\frac{n+1}{2\pi e}} \, (\det L)^{1/n+1}$

$= \sqrt{\frac{n+1}{2\pi e}} \, (2^n S)^{1/n+1}$

$\approx \sqrt{\frac{n+1}{2\pi e}} \, 6 \approx 1.9\sqrt{n}$

$S \approx 2^{2n}$ b/c superincreasing

Approx soln to SVP should still be $\|\vec{t}\|$.

Can make better by using

$(CM_1, CM_2, \dots, CM_n)$ and CS

for large C.