MATH 567: Lecture 27 (04/17/2025)

Today: * LLL reduction
* Hermite Normal Form (HNF)

Lenstra-Lenstra-Lovász (LLL) Reduction (1982) (A.K. Lenstra, H.W. Lenstra)

Let $B=[\bar{b}_1,\dots,\bar{b}_n]$ and $B^*=[\bar{b}_1^*,\dots,\bar{b}_n^*] = GSO(B)$.

B is **LLL-reduced** if

(1) $|\mu_{ij}| \le \frac{1}{2}$ for $1 \le j < i \le n$, and

(2) $\|\bar{b}_i^*\|^2 \le \frac{4}{3} \|\bar{b}_{i+1}^* + \mu_{i+1,i}\bar{b}_i^*\|^2$ for $i=1,\dots,n-1$.

$\rightarrow$ can replace by $1+\varepsilon$ for any $\varepsilon > 0$.

Condition (1) says that $\bar{b}_i$s are "nearly orthogonal". Recall that the GSO coefficient μ_{ij} gives the length of the component/projection of $\bar{b}_i$ along $\bar{b}_j^*$. Having an upper bound of $\frac{1}{2}$ on $|\mu_{ij}|$ specifies that these components are not too large.

Condition (2) says that the $\bar{b}_i$'s are "relatively short". With just condition (1), we could have nearly orthogonal vectors, but $\|\bar{b}_1\|$ could be huge. And even though the $\bar{b}_i$ for $i \ge 2$ are "spread out" according to condition (1) they could all have large norms! Notice that $\bar{b}_{i+1}^* + \mu_{i+1,i}\bar{b}_i^*$ is the component of $\bar{b}_{i+1}$ orthogonal to $\bar{b}_1^*,\dots,\bar{b}_{i-1}^*$, and $\bar{b}_i^*$ is the component of b_i orthogonal to $\bar{b}_1^*,\dots,\bar{b}_{i-1}^*$. The factor $\frac{4}{3}$ ensures the LLL-reduction runs in polynomial time — but it could be replaced by $1+\varepsilon$ for any $\varepsilon > 0$.

Properties of LLL-reduced basis

Recall, $B = [\bar{b}_1, \dots, \bar{b}_n]$, $B^* = GSO(B)$.

(i) $\|\bar{b}_i^*\|^2 \leq 2^{j-i} \|\bar{b}_j^*\|^2 \;\forall\; 1 \leq i < j \leq n$.

(ii) $\|\bar{b}_1^*\| = \|\bar{b}_1\| \leq 2^{(n-1)/4} [\det(\mathcal{L})]^{1/n}$, where

$$\det(\mathcal{L}) = \prod_{j=1}^{n} \|\bar{b}_j^*\| \quad \text{(determinant of lattice } \mathcal{L}\text{)}$$

When $m=n$, and $\bar{b}_j$ are rational, $\det(\mathcal{L}) = \sqrt{\det(B^T B)}$.

(iii) $\|\bar{b}_1^*\| = \|\bar{b}_1\| \leq 2^{(n-1)/2} \lambda(\mathcal{L})$. $\longrightarrow$ length of a shortest vector in $\mathcal{L}$.

(iv) $\|\bar{b}_1\| \cdots \|\bar{b}_n\| \leq 2^{n(n-1)/4} \det(\mathcal{L})$.

Proof of (i)

(i) $\|\bar{b}_i^*\|^2 \leq 2^{j-i} \|\bar{b}_j^*\|^2$, $j > i$.

Condition (2) of LLL-reduction $\Rightarrow$

$$\frac{3}{4}\|\bar{b}_i^*\|^2 \leq \|\bar{b}_{i+1}^* + \mu_{i+1,i}\, \bar{b}_i^*\|^2$$

$$\leq \|\bar{b}_{i+1}^*\|^2 + (\mu_{i+1,i})^2 \|\bar{b}_i^*\|^2$$

as $\|\bar{a}+\bar{b}\|^2 \leq \|\bar{a}\|^2 + \|\bar{b}\|^2 + \underset{=0}{\cancel{2\langle \bar{a},\bar{b}\rangle}}$

$\bar{b}_{i+1}^* \perp \bar{b}_i^*$

$$\leq \|\bar{b}_{i+1}^*\|^2 + \frac{1}{4}\|\bar{b}_i^*\|^2$$

$\Rightarrow \|\bar{b}_i^*\|^2 \leq 2\|\bar{b}_{i+1}^*\|^2 \quad \forall\, i = 1, \dots, n-1$.

$$\Rightarrow \|\bar{b}_i^*\|^2 \leq 2 \cdot 2 \|\bar{b}_{i+2}^*\|^2 \leq 2^{j-i} \|\bar{b}_j^*\|^2, \forall j > i. \qquad \square$$

Note (iii) $\|\bar{b}_1\| \leq 2^{(n-1)/2} \lambda(\mathcal{L})$

The length of $\bar{b}_1$ is at most an exponential factor off from the length of the SV of $\mathcal{L}$. But in practice $\|\bar{b}_1\|$ is often much closer to $\lambda(\mathcal{L})$ than the exponential bound seems to suggest.

Further, the LLL-algorithm runs in polynomial time. There are efficient implementations available as well — see, e.g., https://libntl.org/.

Hermite Normal Form (HNF)

Let $P = \{\bar{x} \in \mathbb{R}^n \mid A\bar{x} = \bar{b}, \bar{x} \geqslant \bar{0}\}$, $A \in \mathbb{Z}^{m \times n}$, $\bar{b} \in \mathbb{Z}^m$.

Q: Is $P \cap \mathbb{Z}^n = \phi$?

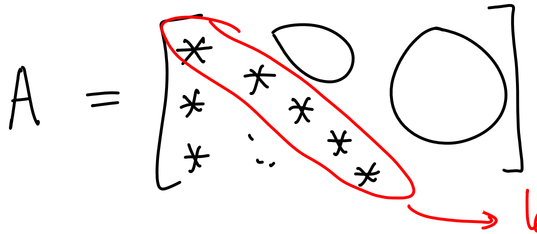
This is the IP feasibility problem, and is NP-complete.

But if we remove $\bar{x} \geqslant \bar{0}$ from the definition of P, the problem is solvable in poly-time.

$\{\bar{x} \mid A\bar{x} = \bar{b}, \bar{x} \in \mathbb{Z}^n\}$: system of linear Diophantine equations.

Def Let $A \in \mathbb{Z}^{m\times n}$ with $\operatorname{rank}(A) = m$. A is in Hermite normal form (HNF) if $A = [B\ 0]$ where $B \in \mathbb{Z}^{m\times m}$ is

1. non-singular $(\det(B) \neq 0)$,
2. non-negative,
3. lower-triangular, and
4. every row of B has a unique maximum entry located on the main diagonal, i.e., $B_{ii} > B_{ij}\ \forall j$.



$*$ = (can be) non-zero

largest in each row, >0.

e.g., $A = \Big[\underbrace{\begin{matrix}2 & 0\\ 1 & 3\end{matrix}}_{B}\ \begin{matrix}0\\ 0\end{matrix}\Big]$ is in HNF.

A can be converted to HNF using elementary column operations (ECOs). With $A = [\bar{a}_1 \cdots \bar{a}_n] \in \mathbb{Z}^{m\times n}$, the ECOs are

1. $\bar{a}_i \rightleftarrows \bar{a}_j$ (swap two columns),
2. $\bar{a}_i \leftarrow -\bar{a}_i$ (scale column by -1), and
3. $\bar{a}_i \leftarrow \bar{a}_i + \lambda \bar{a}_j$, $\lambda \in \mathbb{Z}$ (add integer multiple of column j to column i)

$\mathrm{HNF}([5\ 2]) = [1\ 0]$

$\mathrm{HNF}([6\ 2]) = [2\ 0]$

If $\alpha_i \in \mathbb{Z}$, then $\mathrm{HNF}([\alpha_1\ \alpha_2 \cdots \alpha_n]) = [\gcd(\alpha_1,\ldots,\alpha_n)\ 0 \cdots 0]$.

Example

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{bmatrix} \xrightarrow[C_3-3C_1]{C_2-2C_1} \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \\ 7 & -6 & -11 \end{bmatrix} \xrightarrow[\text{then } C_3+2C_2]{-C_2} \begin{bmatrix} 1 & 0 & 0 \\ 4 & 3 & 0 \\ 7 & 6 & 1 \end{bmatrix}$$

$$\xrightarrow{C_1-C_2} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \\ 1 & 6 & 1 \end{bmatrix} \xrightarrow[C_2-6C_3]{C_1-C_3} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

→ is in HNF!

Theorem 18 (Theorem 4.1 from Schrijver TLIP): A can be brought into HNF using ECO's. The numbers stay bounded in the process.

Proof (of first statement) Suppose (after some steps)

$$A = \begin{array}{c} \\ k \end{array} \begin{bmatrix} \overset{\longleftarrow k \longrightarrow}{B} & O \\ C & D \end{bmatrix}$$

with $B_{k\times k}$ lower triangular, and $\operatorname{diag}(B) > 0$.

$[d_{11}\; d_{12} \cdots d_{1\ell}]$, $\ell = n-k$

We can use ECOs to ensure that

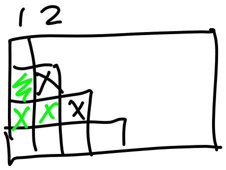
(i) the first row of $D = [d_{11} \cdots d_{1\ell}]$ is ≥ 0, and

(ii) $d_{11} + d_{12} + \cdots + d_{1\ell}$ is minimal.

In fact, we can get $d_{11} > 0$, and $d_{1j} = 0$, $j = 2, \ldots, \ell$.

Hence we have increased the size of B to $(k+1)\times(k+1)$.

Can use further ECOs to get diagonal dominance property.



Use column 2 to make (2,1)-entry "okay".

Then use column 3 to make Row 3 "okay"!

And so on… □

"Farkas' lemma" for IP

$\{A\bar{x} \leq \bar{b}\}$ is infeasible $\Longrightarrow \exists\, \bar{u} \geq \bar{0}$ s.t. $\bar{u}^T A = \bar{0}$, $\bar{u}^T \bar{b} = -1$.

As an application of HNF, we present a Farkas' lemma-type systems of alternatives result for IP.

(1) $\{A\bar{x} = \bar{b}, \bar{x} \in \mathbb{Z}^n\}$ has no solution.
$(A \in \mathbb{Z}^{m \times n}, \ \bar{b} \in \mathbb{Z}^m)$

(2) $\exists\, \bar{y}$ rational such that $\bar{y}^T A$ is integral, $\bar{y}^T \bar{b}$ is non-integral.

"Farkas' lemma" for IP: $(1) \equiv (2)$.

Proof $(2) \Rightarrow (1)$: $\bar{y}^T (A\bar{x} = \bar{b}) \Rightarrow \underbrace{(\bar{y}^T A)}_{\in \mathbb{Z}^n} \bar{x} = \underbrace{\bar{y}^T \bar{b}}_{\notin \mathbb{Z}} \Rightarrow \bar{x} \notin \mathbb{Z}^n$.

$(1) \Rightarrow (2)$: We use HNF(A):

Note that (1) and (2) are both invariant under ECOs. Hence we can assume WLOG that A is in HNF. With HNF(A) = [B 0], where B is non-singular, we get the following result.

$B^{-1}\underbrace{[B\ \ 0]}_{A} = [I\ \ 0]$, i.e., $B^{-1}A$ is integral.

$$B^{-1}(A\bar{x}=\bar{b}) \Rightarrow \underbrace{(B^{-1}A)}_{\in \mathbb{Z}^{m\times n}}\bar{x} = B^{-1}\bar{b}.$$

$(1) \Rightarrow B^{-1}\bar{b} \notin \mathbb{Z}^m$, i.e., with $\bar{u} = B^{-1}\bar{b}$, there is at least one i such that $u_i \notin \mathbb{Z}$. We can choose $\bar{y}^T$ as the i^{th} row of B^{-1}, and we get (2).

□

Note: HNF(A) can be computed in polynomial time, without any A_{ij} becoming too big.