MATH 567: Lecture 26 (04/15/2025)

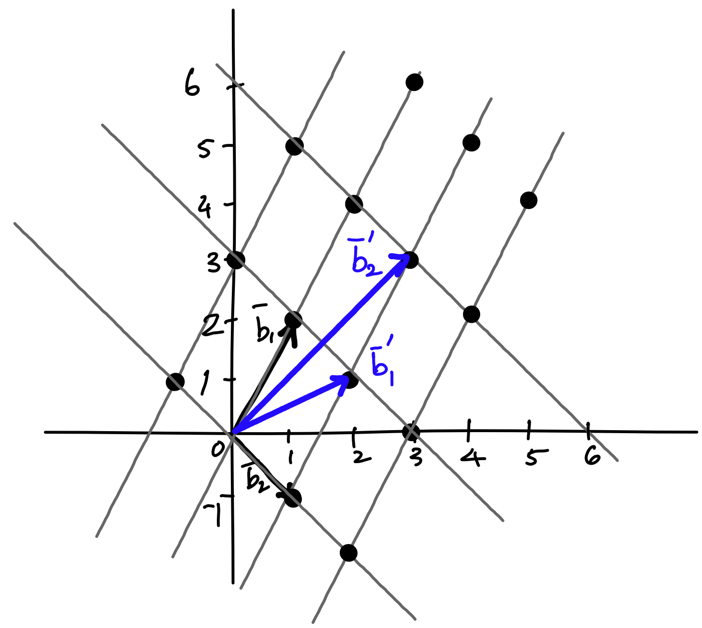
Today: * lattices and basis reduction

Recall: The lattice generated by $B \in \mathbb{R}^{m \times n}$ is $\mathcal{L}(B) = \{B\bar{x} \mid \bar{x} \in \mathbb{Z}^n\}$.
Here, B is a basis for the lattice.

In the example, we had $\mathcal{L}(B) = \mathcal{L}(B')$ with

$$B = [\bar{b}_1 \ \bar{b}_2] = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix} \quad \text{and}$$

$$B' = [\bar{b}_1', \bar{b}_2'] = \begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix}.$$



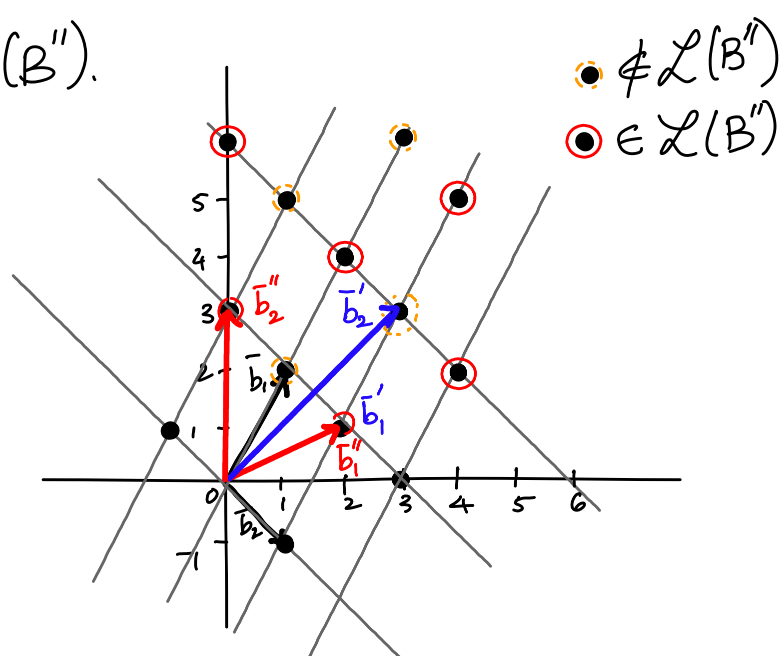
Note: $B' = BU$ where $U = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$.

$$\underbrace{\begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix}}_{B'} = \underbrace{\begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}}_{B} \underbrace{\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}}_{U}. \quad \det(U) = -1.$$

Now, consider $\bar{b}_1'' = \bar{b}_1 + \bar{b}_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and $\bar{b}_2'' = \bar{b}_1 - \bar{b}_2 = \begin{bmatrix} 0 \\ 3 \end{bmatrix}$.

With $B'' = [\bar{b}_1'' \ \bar{b}_2'']$, we see that $\mathcal{L}(B'') \subset \mathcal{L}(B)$,

as $\bar{b}_1 \in \mathcal{L}(B)$, but $\bar{b}_1 \notin \mathcal{L}(B'')$.



Note that $\bar{b}_1 = \frac{1}{2}(\bar{b}_1'' + \bar{b}_2'')$,
and hence we cannot express $\bar{b}_1$ as an integer linear combination of $\bar{b}_1''$ and $\bar{b}_2''$.

$\mathcal{L}(B'')$ is a **sublattice** of $\mathcal{L}(B)$.

Two fundamental problems in lattices

1. Shortest Vector Problem (SVP): Given a basis $B \in \mathbb{Z}^{m \times n}$ for lattice $\mathcal{L}(B)$, find $\bar{x} \in \mathbb{Z}^n / \{\bar{0}\}$ such that $\|B\bar{x}\| \le \|B\bar{y}\| \;\; \forall \; \bar{y} \in \mathbb{Z}^n / \{\bar{0}\}$.

   Euclidean norm

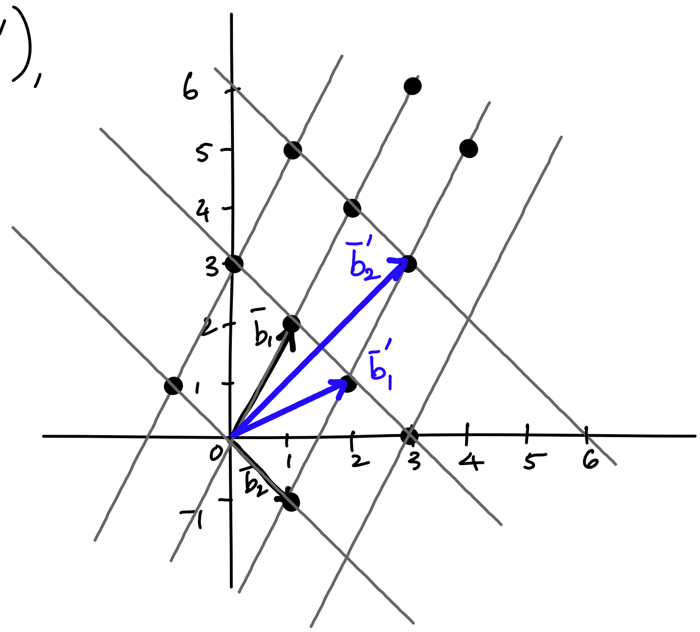
In words, find shortest nonzero vector in $\mathcal{L}(B)$.

2. Closest Vector Problem (CVP) Given a basis $B \in \mathbb{Z}^{m \times n}$ and a target vector $\bar{t} \in \mathbb{R}^m$, find $\bar{x} \in \mathbb{Z}^n$ such that

   $\|B\bar{x} - \bar{t}\| \le \|B\bar{y} - \bar{t}\| \;\; \forall \; \bar{y} \in \mathbb{Z}^n$.

In words, find the closest vector in $\mathcal{L}(B)$ to $\bar{t}$ (could be $\bar{0}$).

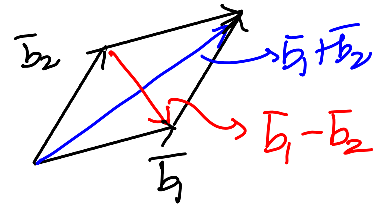
With $B = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}$, $\bar{b}_2 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$ is a shortest vector of $\mathcal{L}(B)$. $\bar{b}_2$ is also a shortest vector of $\mathcal{L}(B')$, as $\mathcal{L}(B') = \mathcal{L}(B)$.



SVP in 2D can be solved in polynomial time by Gauss Reduction.

Def $B = [\bar{b}_1\ \bar{b}_2]$ with $\bar{b}_1, \bar{b}_2 \in \mathbb{Z}^2$ is **reduced** if

$$\|\bar{b}_1\|, \|\bar{b}_2\| \leq \|\bar{b}_1 + \bar{b}_2\|, \|\bar{b}_1 - \bar{b}_2\|.$$



The sides of the parallelogram are not longer than its diagonals.

$\bar{b}_1$ in a reduced basis will be a shortest vector of $\mathcal{L}(B)$.

We present the standard notion of orthogonalization in $\mathbb{R}^m$ — we will use it as a guide for reduction using integer multipliers.

Gram-Schmidt Orthogonalization (GSO) (in $\mathbb{R}^m$)

$B = [\bar{b}_1, \ldots, \bar{b}_n]$, $\bar{b}_j \in \mathbb{R}^m\ \forall j$

$B^* = GSO(B)$

$\bar{b}_1^* = \bar{b}_1$;

for $i = 1, \ldots, n$

$$\bar{b}_i^* = \bar{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \bar{b}_j^*$$

end

where $\mu_{ij} = \dfrac{\bar{b}_i^T \bar{b}_j^*}{\|\bar{b}_j^*\|^2} \left(\text{or } \dfrac{\langle \bar{b}_i, \bar{b}_j^* \rangle}{\|\bar{b}_j^*\|^2} \right)$ for $j < i$, and

$$\mu_{ii} = 1\ \forall i, \quad \mu_{ij} = 0\ \forall j > i.$$

μ_{ij} = length of component of $\bar{b}_i$ in direction of $\bar{b}_j^*$.

Gauss Reduction (in 2D)

$[\tilde{\bar{b}}_1 \; \tilde{\bar{b}}_2] = \text{GAUSS}(\bar{b}_1, \bar{b}_2);$ input: $\bar{b}_1, \bar{b}_2 \in \mathbb{Z}^2$

do

  if $\|\bar{b}_1\| > \|\bar{b}_2\|$

    swap$(\bar{b}_1, \bar{b}_2)$;

  end-if

  $\mu = \left\lfloor \dfrac{\langle \bar{b}_2, \bar{b}_1 \rangle}{\|\bar{b}_1\|^2} \right\rceil;$

  $\bar{b}_2 = \bar{b}_2 - \mu \bar{b}_1;$

  if $\|\bar{b}_1\| \leq \|\bar{b}_2\|$

    return$([\bar{b}_1, \bar{b}_2])$;

    break; $\longrightarrow$ this terminates the algorithm

  end-if

while $(\|\bar{b}_1\| > \|\bar{b}_2\|)$

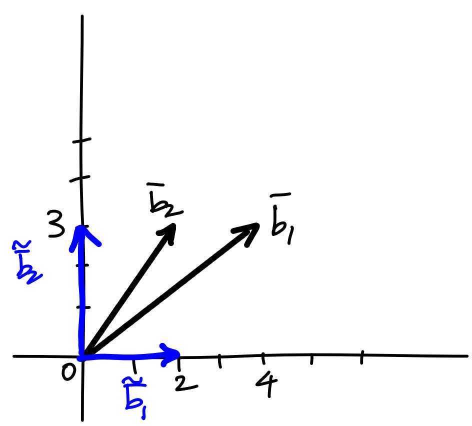
Example

$$B = [\bar{b}_1 \; \bar{b}_2] = \begin{array}{cc} \bar{b}_1 & \bar{b}_2 \\ \end{array}\begin{bmatrix} 4 & 2 \\ 3 & 3 \end{bmatrix}$$

1. $\|\bar{b}_2\| < \|\bar{b}_1\| \Rightarrow$ swap$(\bar{b}_1, \bar{b}_2)$

$$\mu = \left\lfloor \frac{\langle \bar{b}_2, \bar{b}_1 \rangle}{\|\bar{b}_1\|^2} \right\rceil = \left\lfloor \frac{17}{13} \right\rceil = 1.$$

$$\bar{b}_2 = \bar{b}_2 - \mu \bar{b}_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}.$$



2. $B = \begin{array}{cc} \bar{b}_1 & \bar{b}_2 \end{array}\begin{bmatrix} 2 & 2 \\ 3 & 0 \end{bmatrix}.$

swap $\Longrightarrow$ $B = \begin{bmatrix} 2 & 2 \\ 0 & 3 \end{bmatrix}.$

$\mu = \left\lfloor \frac{4}{4} \right\rceil = 1.$ $\bar{b}_2 = \begin{bmatrix} 2 \\ 3 \end{bmatrix} - \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 3 \end{bmatrix}.$

But, finding a shortest vector in $n \geq 3$ dimensions is hard!

$\tilde{B} = B = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}.$ $\tilde{\bar{b}}_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$ is a shortest vector in $\mathcal{L}(B)$.

We now define reduced bases in higher dimensions.

Reduced bases for $n \geq 3$

We need some more notation.

Let $\bar{b}_i(l) = \sum_{j=l}^{n} \mu_{ij} \bar{b}_j^*$

$\bar{b}_i(l)$ is the component of $\bar{b}_i$ orthogonal to $\bar{b}_1^*, \bar{b}_2^*, \ldots, \bar{b}_{l-1}^*$.

Also, let $\mathcal{L}_i = \mathcal{L}([\bar{b}_i(i), \ldots, \bar{b}_n(i)])$.

e.g., $\bar{b}_{i+1}(i) = \mu_{i+1,i} \bar{b}_i^* + \bar{b}_{i+1}^*$, which is the component of $\bar{b}_{i+1} \perp \bar{b}_1^*, \bar{b}_2^*, \ldots, \bar{b}_{i-1}^*$.

Korkine-Zolotarev (KZ) reduction

$B = [\bar{b}_1, \ldots, \bar{b}_n]$ is KZ-reduced if

* $\bar{b}_1$ is an SV of $\mathcal{L}(B)$; shortest vector
* for $i \geq 2$
  $\bar{b}_i(i)$ is an SV of $\mathcal{L}_i$.

Notice that Gauss reduction $\equiv$ KZ-reduction in 2D.

Thus, KZ-reduction specifies quite a strong condition for a basis's being reduced, as the shortest vector conditions are imposed on larger and larger subsets of vectors (and not just on pairs of them).

If B is KZ-reduced, then

$$\frac{4}{i+3} \leq \frac{\|\bar{b}_i\|^2}{\lambda_i^2(\mathcal{L})} \leq \frac{i+3}{4}, \text{ for } i=1,\ldots,n$$

where $\lambda_i(\mathcal{L})$ = length of a shortest vector in $\mathcal{L}_i$.

Thus for $i=1$, $\|b_1\| = \lambda_1(\mathcal{L}) = \lambda(\mathcal{L})$, i.e., $\bar{b}_1$ is an SV of $\mathcal{L}(B)$.

For $i \geq 2$, $\|b_i\|$ is at most $\sqrt{n}$ off from λ_i, the i^{th} minimum of the lattice.

While KZ-reduction is strong in its enforcement, computing a KZ-reduced basis starting from any basis is hard (no polynomial time algorithm is known). We consider less strict definitions that could be computed efficiently.

We first give an equivalent definition of Gauss reduction using the GSO coefficients μ_{ij}. This definition can be more easily extended to higher dimensions.

Equivalent definition of Gauss reduction:

$B = [\bar{b}_1, \bar{b}_2]$ is Gauss-reduced if

$$\|\bar{b}_1\|^2 \leq \|\bar{b}_2\|^2$$

and $$\left| \frac{\langle \bar{b}_2, \bar{b}_1 \rangle}{\|\bar{b}_1\|^2} \right| \leq \frac{1}{2}.$$

We will round $\frac{1}{2}$ to 0. With this assumption, $\lfloor \mu \rceil = 0$.