LLL Overview

Lenstra-Lenstra-Lovász lattice basis reduction

Curtis Bright

July 31, 2008

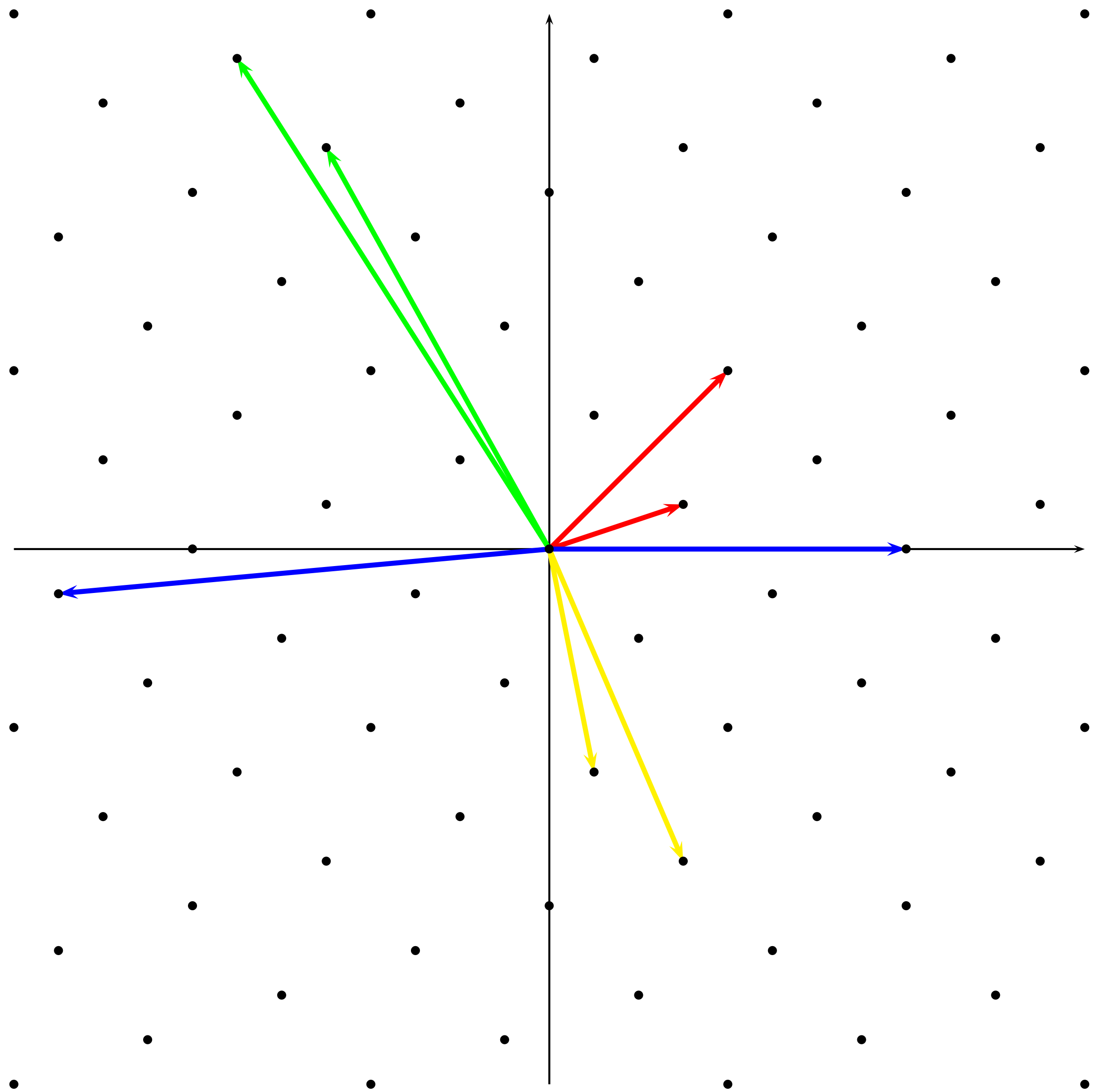
Lattices

- Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be linearly independent vectors in $\mathbb{R}^n$.

- The lattice $L \subset \mathbb{R}^n$ generated by $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is:

$$L = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \;\middle|\; x_i \in \mathbb{Z} \right\}$$

- $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ is a basis of L. When $n > 1$, infinitely many bases exist.



Lattice Volume

- The basis vectors form an n-dimensional parallelotope:

$$P = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \;\middle|\; x_i \in [0, 1) \right\}$$

- Define vol(L) to be the volume of P:

$$\text{vol}(L) = |\det(\mathbf{b}_1\, \mathbf{b}_2\, \cdots\, \mathbf{b}_n)|$$

- This is independent of the choice of basis of L.

Theorem (Hadamard's Inequality). *Let* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *be a basis of* L. *Then*

$$\mathsf{vol}(L) \leq \prod_{i=1}^{n} \|\mathbf{b}_i\|$$

with equality if and only if the basis vectors are orthogonal.

- Intuitively, the amount of nonorthogonality of a basis is measured by $\prod_{i=1}^{n} \|\mathbf{b}_i\|$.

Hermite's Constant(s)

Theorem (Hermite). *There exists a constant* γ_n *such that all lattices of dimension* n *have some basis* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *which satisfies*

$$\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq \sqrt{\gamma_n}^{\,n}\, \mathrm{vol}(L).$$

- Langrage had previously given an algorithm to find a basis $\mathbf{b}_1, \mathbf{b}_2$ of any lattice $L \subset \mathbb{R}^2$ such that

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \leq \sqrt{4/3}\, \mathrm{vol}(L).$$

  Thus, $\gamma_2 \leq \sqrt{4/3}$.

Langrage's Algorithm

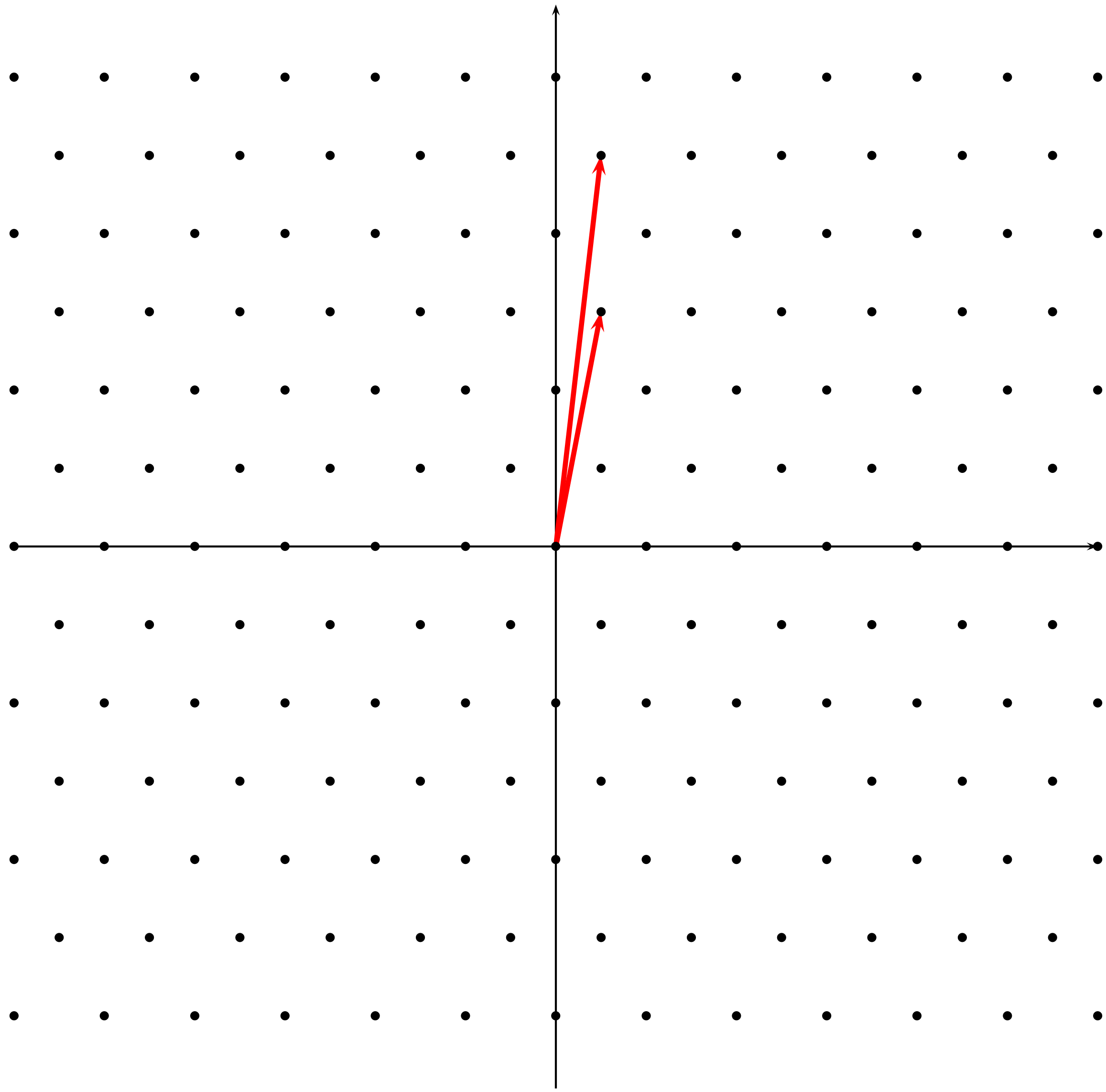
Input: A basis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^2$ for lattice L with $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$

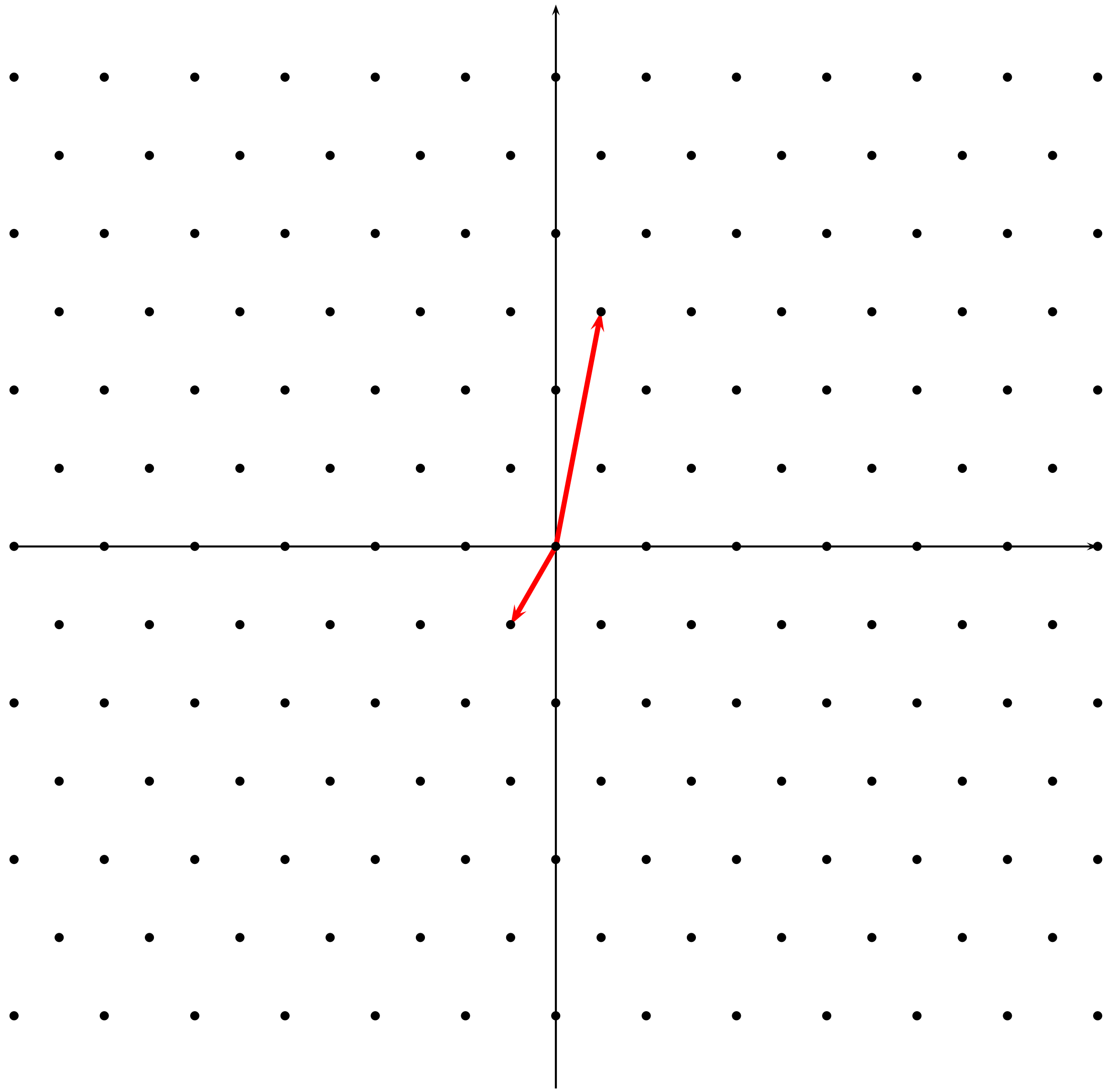
Output: A basis of L with $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ and $|\mathbf{b}_1 \cdot \mathbf{b}_2| \leq \|\mathbf{b}_1\|^2 / 2$

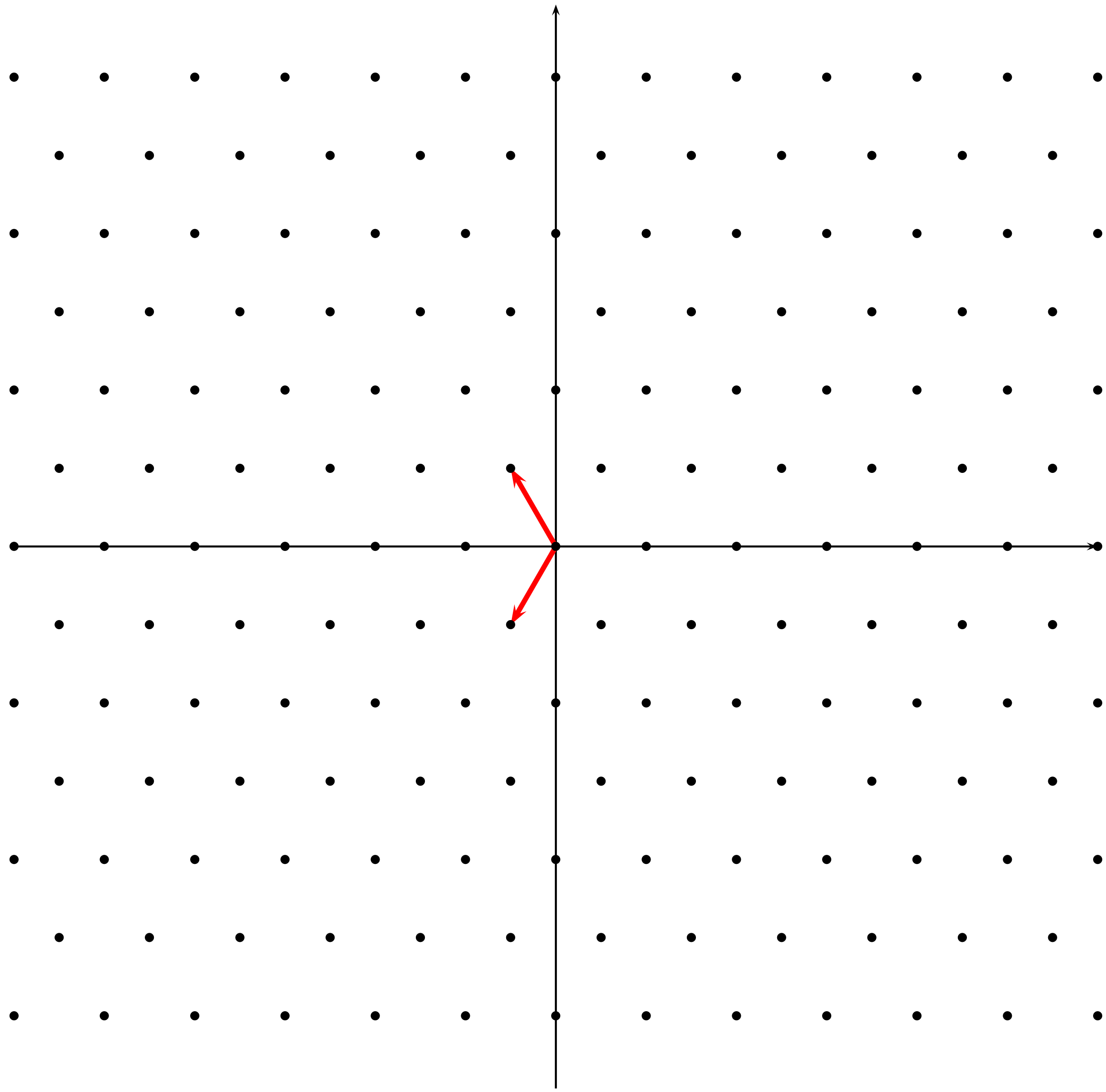
REPEAT:

Add multiples of $\mathbf{b}_1$ to $\mathbf{b}_2$ to minimize the projection of $\mathbf{b}_2$ on $\mathbf{b}_1$

IF $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ THEN RETURN $\mathbf{b}_1, \mathbf{b}_2$







- We have $\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| = \sqrt{4/3}\,\mathrm{vol}(L)$ for the basis we just found, and by inspection we see $\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\|$ cannot be decreased: therefore

$$\gamma_2 = \sqrt{4/3}.$$

- Hermite generalized this algorithm to find bases $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of any lattice $L \subset \mathbb{R}^n$ such that

$$\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq \sqrt{\gamma_2^{n-1}}^{\,n}\,\mathrm{vol}(L).$$

  Thus, $\gamma_n \leq \gamma_2^{n-1}$.

- In fact, $\gamma_n \in \Theta(n)$: for large n, $\frac{n}{2\pi e} < \gamma_n < \frac{n}{\pi e}$.

Basis Reduction

- Bases with short vectors are easier to work with.

- The best possible basis would have $\mathbf{b}_1$ as the shortest nonzero vector in the lattice and in general $\mathbf{b}_i$ as the shortest nonzero vector such that $\mathbf{b}_1, \ldots, \mathbf{b}_i$ is linearly independent.

- Unfortunately, in general finding the shortest nonzero vector of a lattice is an NP-hard problem.

- And it is unknown if the running time of Hermite's generalized algorithm is polynomial in n.

- However, relaxing some of the requirements on the basis will enable us to give an algorithm which is polynomial time in n.

Relaxed Basis Conditions

- Reducing the vector lengths $\|\mathbf{b}_i\|$ will also reduce $\prod_{i=1}^{n} \|\mathbf{b}_i\|$: good bases tend to be approximately orthogonal.

- We will therefore try to minimize *shortness* and *nonorthogonality*.

  - Minimize the projection of $\mathbf{b}_i$ on span$(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$.

  - Roughly speaking, enforce a condition $\|\mathbf{b}_i\| \geq \frac{1}{2} \|\mathbf{b}_{i-1}\|$.

The Gram-Schmidt Process

- Given a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ for $\mathbb{R}^n$, the Gram-Schmidt process finds a orthogonal basis $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ for $\mathbb{R}^n$ [not L].

- Define $\text{proj}_{\mathbf{u}}\, \mathbf{v} = \frac{\mathbf{v} \cdot \mathbf{u}}{\mathbf{u} \cdot \mathbf{u}} \mathbf{u}$.

- The orthogonal basis of $\mathbb{R}^n$ is computed as follows:

$$\begin{aligned}
\mathbf{b}_1^* &= \mathbf{b}_1 \\
\mathbf{b}_2^* &= \mathbf{b}_2 - \text{proj}_{\mathbf{b}_1^*}\,\mathbf{b}_2 \\
\mathbf{b}_3^* &= \mathbf{b}_3 - \text{proj}_{\mathbf{b}_1^*}\,\mathbf{b}_3 - \text{proj}_{\mathbf{b}_2^*}\,\mathbf{b}_3 \\
\mathbf{b}_4^* &= \mathbf{b}_4 - \text{proj}_{\mathbf{b}_1^*}\,\mathbf{b}_4 - \text{proj}_{\mathbf{b}_2^*}\,\mathbf{b}_4 - \text{proj}_{\mathbf{b}_3^*}\,\mathbf{b}_4 \\
&\vdots \\
\mathbf{b}_i^* &= \mathbf{b}_i - \sum_{j=1}^{i-1} \text{proj}_{\mathbf{b}_j^*}\,\mathbf{b}_i
\end{aligned}$$

- Intuitively, $\mathbf{b}_i^* = \text{proj}_{\text{span}(\mathbf{b}_1,\ldots,\mathbf{b}_{i-1})^\perp}\,\mathbf{b}_i$.

- Let $\mu_{i,j}$ be the coefficient used in $\text{proj}_{\mathbf{b}_j^*}\,\mathbf{b}_i$, i.e., $\mu_{i,j} = \frac{\mathbf{b}_i \cdot \mathbf{b}_j^*}{\mathbf{b}_j^* \cdot \mathbf{b}_j^*}$.

- It is likely $\mu_{i,j} \notin \mathbb{Z}$, so likely $\mathbf{b}_i^* \notin L$ for $i > 1$.

Vector Size Reduction

- We can't use $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ as a basis for L, but we can modify the Gram-Schmidt process so that all coefficients used will be integers:

$$\begin{aligned}
\mathbf{b}_1 &:= \mathbf{b}_1 \\
\mathbf{b}_2 &:= \mathbf{b}_2 - \lceil \mu_{2,1} \rfloor \mathbf{b}_1 \\
\mathbf{b}_3 &:= \mathbf{b}_3 - \lceil \mu_{3,1} \rfloor \mathbf{b}_1 - \lceil \mu_{3,2} \rfloor \mathbf{b}_2 \\
\mathbf{b}_4 &:= \mathbf{b}_4 - \lceil \mu_{4,1} \rfloor \mathbf{b}_1 - \lceil \mu_{4,2} \rfloor \mathbf{b}_2 - \lceil \mu_{4,3} \rfloor \mathbf{b}_3 \\
&\vdots \\
\mathbf{b}_i &:= \mathbf{b}_i - \sum_{j=i-1}^{1} \lceil \mu_{i,j} \rfloor \mathbf{b}_j
\end{aligned}$$

- Then the new values of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ will be a basis for L with $\left|\mu_{i,j}\right| \leq \frac{1}{2}$ for all $i > j$. Such a basis is called *size-reduced*.

Lovász Condition

- It is preferable to have $\left\|\mathbf{b}_n^*\right\| \geq \left\|\mathbf{b}_{n-1}^*\right\| \geq \cdots \geq \left\|\mathbf{b}_1^*\right\|$.

- Hermite showed every lattice has a size-reduced basis such that $\left\|\mathbf{b}_i^*\right\| \geq \frac{1}{\gamma_2}\left\|\mathbf{b}_{i-1}^*\right\|$ for $2 \leq i \leq n$. (But without an efficient way to find such a basis. . .)

- Instead, LLL uses a relaxed version known as the *Lovász Condition*:

$$\left\|\mathbf{b}_i^* + \mathrm{proj}_{\mathbf{b}_{i-1}^*}\mathbf{b}_i\right\| \geq \frac{1}{\gamma_2}\left\|\mathbf{b}_{i-1}^*\right\|$$

LLL Algorithm

Input: A basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$ for lattice L

Output: A basis of L which is size-reduced and satisfies the Lovász Condition

Initialization: $k := 2$; Compute GSO ($\mathbf{b}_i^*$ and $\mu_{i,j}$)

WHILE $k \leq n$ DO

  FOR i FROM $k-1$ TO 1 DO

    $\mathbf{b}_i := \mathbf{b}_i - \lceil \mu_{k,i} \rfloor \mathbf{b}_i$

    $\mu_{k,j} := \mu_{k,j} - \lceil \mu_{k,i} \rfloor \mu_{i,j}$ for $j \leq i$

  IF Lovász Condition is satisfied (or $k = 1$) THEN

    $k := k + 1$

  ELSE

    Swap $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$ and update GSO

    $k := k - 1$

RETURN $\mathbf{b}_1, \ldots, \mathbf{b}_n$

LLL-reduced Basis Properties

$$\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq \sqrt{\sqrt{2}^{n-1}}^{\,n} \text{vol}(L)$$

- Thus $\gamma_n \leq 1.41^{n-1}$ (Hermite's Algorithm gave $\gamma_n \leq 1.15^{n-1}$).

- Also, some $\mathbf{b}_i$ will satisfy

$$\|\mathbf{b}_i\| \leq \sqrt{2}^{n-2} \lambda_1(L)$$

where $\lambda_1(L)$ is the shortest nonzero vector of L.