Gram-Schmidt Algorithm

Suppose $\mathcal{B} = \{\vec{\mathbf{v_1}}, \vec{\mathbf{v_2}}, \ldots, \vec{\mathbf{v_n}}\}$ is the basis for an subspace $S \subset \mathbb{R}^m$.

Form the set $\mathcal{B}^* = \{\vec{\mathbf{v_1}}^*, \vec{\mathbf{v_2}}^*, \ldots, \vec{\mathbf{v_n}}^*\}$ by

$$\begin{aligned}
\vec{\mathbf{v_1}}^* &= \vec{\mathbf{v_1}} \\
\vec{\mathbf{v_2}}^* &= \vec{\mathbf{v_2}} - \frac{\vec{\mathbf{v_2}} \cdot \vec{\mathbf{v_1}}^*}{\vec{\mathbf{v_1}}^* \cdot \vec{\mathbf{v_1}}^*}\vec{\mathbf{v_1}}^* \\
\vec{\mathbf{v_3}}^* &= \vec{\mathbf{v_3}} - \frac{\vec{\mathbf{v_3}} \cdot \vec{\mathbf{v_2}}^*}{\vec{\mathbf{v_2}}^* \cdot \vec{\mathbf{v_2}}^*}\vec{\mathbf{v_2}}^* - \frac{\vec{\mathbf{v_3}} \cdot \vec{\mathbf{v_1}}^*}{\vec{\mathbf{v_1}}^* \cdot \vec{\mathbf{v_1}}^*}\vec{\mathbf{v_1}}^* \\
&\vdots \\
\vec{\mathbf{v_i}}^* &= \vec{\mathbf{v_i}} - \sum_{j=1}^{i-1} \mu_{i,j}\vec{\mathbf{v_j}}^* \qquad \text{where } \mu_{i,j} = \frac{\vec{\mathbf{v_i}} \cdot \vec{\mathbf{v_j}}^*}{\vec{\mathbf{v_j}}^* \cdot \vec{\mathbf{v_j}}^*}, \quad 1 \leq j < i
\end{aligned}$$

Then $\mathcal{B}^*$ is an orthogonal basis for S.

Proposition 7.66 (Gaussian Lattice Reduction)

Let $L \subset \mathbb{R}^2$ be a lattice with basis $\mathcal{B} = \{\vec{\mathbf{v_1}}, \vec{\mathbf{v_2}}\}$.

The following algorithm terminates and yields a good basis for L:

- If $\|\vec{\mathbf{v_2}}\| < \|\vec{\mathbf{v_1}}\|$ then swap $\vec{\mathbf{v_1}}$ and $\vec{\mathbf{v_2}}$
- Compute $m = \left\lfloor \dfrac{\vec{\mathbf{v_1}} \cdot \vec{\mathbf{v_2}}}{\vec{\mathbf{v_1}} \cdot \vec{\mathbf{v_1}}} \right\rceil$
- If $m = 0$, then $\mathcal{B}' = \{\vec{\mathbf{v_1}}, \vec{\mathbf{v_2}}\}$ is a good basis
- If $m \neq 0$, then assign $\vec{\mathbf{v_2}} = \vec{\mathbf{v_2}} - m\vec{\mathbf{v_1}}$ and repeat the loop

When the loop terminates, $\vec{\mathbf{v_1}}$ is the shortest vector in L so this solves the SVP.

Further, $\mathcal{B}'$ is quasi-orthogonal, where θ, the angle between $\vec{\mathbf{v_1}}$ and $\vec{\mathbf{v_2}}$, satisfies $\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$

Definition: LLL Reduced Basis

Let $\mathcal{B} = \{\vec{\mathbf{v_1}}, \ldots, \vec{\mathbf{v_n}}\}$ be a basis for the lattice $L \subset \mathbb{R}^n$ and let $\mathcal{B}^* = \{\vec{\mathbf{v_1}}^*, \ldots, \vec{\mathbf{v_n}}^*\}$ be the Gram-Schmidt basis for $\mathcal{B}$.

Then $\mathcal{B}$ is said to be **LLL reduced** if it satisfies the two conditions:

- *Size condition:* $|\mu_{i,j}| \leq \frac{1}{2}$ for all $1 \leq j < i \leq n$
- *Lovàsz Condition:* $\|\vec{\mathbf{v_i}}^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|\vec{\mathbf{v_{i-1}}}^*\|^2$ for all $1 < i \leq n$

Theorems 7.69 & 7.71

Thm 7.69: Let $L \subset \mathbb{R}^n$ be a lattice of dimension n with an LLL reduced basis $\mathcal{B} = \{\vec{\mathbf{v_1}}, \ldots, \vec{\mathbf{v_n}}\}$. Then

$$\prod_{i=1}^{n} \|\vec{\mathbf{v_i}}\| \leq 2^{n(n-1)/4} \det(L)$$

$$\|\vec{\mathbf{v_j}}\| \leq 2^{(i-1)/2} \|\vec{\mathbf{v_i^*}}\| \qquad \text{for all } 1 \leq j \leq i \leq n$$

$$\|\vec{\mathbf{v_1}}\| \leq 2^{(n-1)/2} \min_{\vec{\mathbf{0}} \neq \vec{\mathbf{v}} \in L} \|\vec{\mathbf{v}}\|$$

Theorems 7.69 & 7.71

Thm 7.69: Let $L \subset \mathbb{R}^n$ be a lattice of dimension n with an LLL reduced basis $\mathcal{B} = \{\vec{\mathbf{v_1}}, \ldots, \vec{\mathbf{v_n}}\}$. Then

$$\prod_{i=1}^{n} \|\vec{\mathbf{v_i}}\| \leq 2^{n(n-1)/4} \det(L)$$

$$\|\vec{\mathbf{v_j}}\| \leq 2^{(i-1)/2} \|\vec{\mathbf{v_i^*}}\| \qquad \text{for all } 1 \leq j \leq i \leq n$$

$$\|\vec{\mathbf{v_1}}\| \leq 2^{(n-1)/2} \min_{\vec{\mathbf{0}} \neq \vec{\mathbf{v}} \in L} \|\vec{\mathbf{v}}\|$$

Thm 7.71: The LLL algorithm takes any basis for L and returns an LLL reduced basis in polynomial time.

From Hoffstein, Pipher, Silverman

Input a basis $\{v_1, \ldots, v_n\}$ for a lattice L
Set $k = 2$
Set $v_1^* = v_1$
Loop while $k \le n$
  Loop Down $j = k-1, k-2, \ldots, 2, 1$
    Set $v_k = v_k - \lfloor \mu_{k,j} \rceil v_j$ [Size Reduction]
  End j Loop
  If $\|v_k^*\|^2 \ge \left(\frac{3}{4} - \mu_{k,k-1}^2\right) \|v_{k-1}^*\|^2$ [Lovász Condition]
    Set $k = k + 1$
  Else
    Swap v_{k-1} and v_k [Swap Step]
    Set $k = \max(k-1, 2)$
  End If
End k Loop
Return LLL reduced basis $\{v_1, \ldots, v_n\}$

Note: At each step, $v_1^*, \ldots, v_k^*$ is the orthogonal set of vectors obtained by applying Gram–Schmidt (Theorem 7.13) to the current values of $v_1, \ldots, v_k$, and $\mu_{i,j}$ is the associated quantity $(v_i \cdot v_j^*)/\|v_j^*\|^2$.

Figure 7.8: The LLL lattice reduction algorithm