Definition 1 (Gram-Schmidt) Let $(b_1, \ldots, b_n)$ be a set of linearly independent vectors, then a Gram-Schmidt set can be obtained by setting

- $b_1^* = b_1$
- $b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j$ for $i = 2, \ldots, n$, where $\mu_{i,j} = \dfrac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$.

The length of Gram-Schmidt vectors can be used to determine the degree of orthogonality of a certain basis. More precisely, a lattice basis is "close to orthogonal if the lengths of the Gram-Schmidt vectors do not decrease too rapidly.

Example 1 Two bases for $\mathbb{Z}_2$ are $\{(1,0),(0,1)\}$ and $\{(23,24),(24,25)\}$. In the first case, the Gram-Schmidt vectors both have length 1. In the second case the Gram- Schmidt vectors are $b_1^* = (23,24)$ and $b_2^* = (24/1105, -23/1105)$, which have lengths $\sqrt{1105} \approx 33.24$ and $1\sqrt{1105} \approx 0.03$ respectively. The fact that the lengths of the Gram-Schmidt vectors dramatically decrease reveals that the original basis is not of good quality.

Proposition 1 (Properties of Gram-Schmidt) *Let $\{b_1, \ldots, b_n\}$ be linearly independent in $\mathbb{R}^m$ and let $b_1^*, \ldots, b_n^*$ be the Gram-Schmidt orthogonalisation.*

1. $||b_i^*|| \leq ||b_i||$ *for* $1 \leq i \leq n$.
2. $\langle b_i, b_i^* \rangle = \langle b_i^*, b_i^* \rangle$ *for 1*$\leq i \leq n$.
3. *If* $b_k' = b_k - \lfloor \mu_{k,j} \rceil b_j$ *for 1* $\leq k \leq n$ *and* $1 \leq j < k$ *and if* $\mu_{k,j}' = \dfrac{\langle b_k', b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$ *then* $|\mu_{k,j}'| \leq 1/2$.

Definition 2 (LLL Reduced Basis) Let $\{b_1, \ldots, b_n\}$ be an ordered basis for a lattice. Denote by $\{b_1^*, \ldots, b_n^*\}$ the Gram-Schmidt orthogonalisation and write $B_i = ||b_i^*||^2 = \langle b_i^*, b_i^* \rangle$. Fix $1/4 < \delta < 1$. The (ordered) basis is *LLL reduced* (with factor δ) if the following conditions hold:

- (Size reduced) $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$.
- (Lovász condition) $B_i \geq (\delta - \mu_{i,i-1}^2) B_{i-1}$ for $2 \leq i \leq n$.

It is traditional to choose $\delta = 3/4$ in the Lovász condition.

We now look at some properties of the LLL reduced bases. We need two intermediate lemmas.

Lemma 1 *Let $\{b_1, \ldots, b_n\}$ be an LLL reduced basis with $\delta = 3/4$ for a lattice $L \subset \mathbb{R}^m$. Let the notation be as above. Then:*

1. $B_j \leq 2^{i-j} B_i$ *for* $1 \leq j \leq i \leq n$.
2. $B_i \leq ||b_i||^2 \leq (1/2 + 2^{i-2}) B_i$ *for* $1 \leq i \leq n$.
3. $||b_j|| \leq 2^{(i-1)/2} ||b_i^*||$ *for* $1 \leq j \leq i \leq n$.

Lemma 2 *Let $\{b_1, \ldots, b_n\}$ be an ordered basis for a lattice $L \subset \mathbb{R}^m$ and let $\{b_1^*, \ldots, b_n^*\}$ be the Gram-Schmidt orthogonalisation. Let λ_1 be the length of the shortest non-zero vector in the lattice. Then $\lambda_1 \geq \min_{1 \leq i \leq n} ||b_i^*||$. Furthermore, let $w_1, \ldots, w_i \in L$ be linearly independent lattice vectors such that $\max\{||w_1||, \ldots, ||w_i||\} = \lambda_i$, as in the definition of successive minima. Write $w_j = \sum_{k=1}^{n} z_{j,k} b_k$. For $1 \leq j \leq i$ denote by $k(j)$ the largest value for k such that $1 \leq k \leq n$ and $z_{j,k} \neq 0$. Then $||w_j|| \geq ||b_k^*(j)||$.*

Theorem 1 *Let $\{b_1, \ldots, b_n\}$ be an LLL reduced basis with $\delta = 3/4$ for a lattice $L \subset \mathbb{R}^m$. Let the notation be as above. Then:*

1. $||b_1|| \leq 2^{(n-1)/2} \lambda_1$.
2. $||b_j|| \leq 2^{(n-1)/2} \lambda_i$ *for* $1 \leq j \leq i \leq n$.
3. $2^{(1-i)/2} \lambda_i \leq ||b_i|| \leq 2^{(n-1)/2} \lambda_i$.
4. $\det(L) \leq \prod_{i=1}^{n} ||b_i|| \leq 2^{n(n-1)/4} \det(L)$.
5. $||b_1|| \leq 2^{(n-1)/4} \det(L) 1/n$.

Proof

1. From part 1 of Lemma 1 we know $||b_i^*|| \geq 2^{(i-1)/2} ||b_1^*||$. Hence, we have that part 1 implies $\lambda_1 \geq \min_{1 \leq i \leq n} ||b_i^*|| \geq \min_{1 \leq i \leq n} 2^{(1-i)/2} ||b_1^*|| = 2^{(1-n)/2} ||b_1^*||$. The result follows since $b_1^* = b_1$.

2. Let $w_1, \ldots, w_i \in L$ be linearly independent lattice vectors with $\max\{||w_1||, \ldots, ||w_i||\} = \lambda_i$. Let $k(j)$ be defined as in Lemma 2 so that $||w_j|| \geq ||b_{k(j)}^*||$. Renumber the vectors w_j so that $k(1) \leq k(2) \leq \cdots \leq k(i)$. We claim that $j \leq k(j)$. If not then $w_1, \ldots, w_j$ would belong to the span of $\{b_1, \ldots, b_{j-1}\}$ and would be linearly dependent.
   Finally, $||b_j|| \leq 2^{(k(j)-1)/2} ||b_{k(j)}^*|| \leq 2^{(n-1)/2} ||w_j|| \leq 2^{(n-1)/2} \lambda_i$, which proves the result.

3. The upper bound on $||b_i||$ is given by part 2. Since $\{b_1, \ldots, b_i\}$ are linearly independent we have $\lambda_i \leq \max_{1 \leq j \leq i} ||b_j||$ and by part 3 of Lemma 1 each $||b_j|| \leq 2^{(i-1)/2} ||b_i^*||$. Using $||b_i^*|| \leq ||b_i||$ we obtain the lower bound on $||b_i||$.

4. We know that $\det(L) = \prod_{i=1}^{n} ||b_i^*||$. The result follows from $||b_i^*|| \leq ||b_i|| \leq 2^{(i-1)/2} ||b_i^*||$.

5. By part 3 of Lemma 1 we have $||b_1|| \leq 2^{(i-1)/2} ||b_i^*||$ and so $||b_1||^n \leq \prod_{i=1}^{n} 2^{(i-1)/2} ||b_i^*|| = 2^{n(n-1)/4} \det(L)$. By taking the n-th root on both sides we are done.

Corollary 1 *If* $||b_1|| \leq ||b_i^*||$ *for all* $1 \leq i \leq n$ *then* b_1 *is a correct solution to SVP.*

We can now proceed to describe the LLL algorithm in detail.

Table 1: The LLL Algorithm

Input: $b_1, \ldots, b_n \in \mathbb{Z}^m$
Output: LLL reduced basis $b_1, \ldots, b_n$

Compute the Gram-Schmidt basis $b_1^*, \ldots, b_n^*$ and coefficients $\mu_{i,j}$ for $1 \leq j < i \leq n$
Compute $B_i = \langle b_i^*, b_i^* \rangle = ||b_i^*||^2$ for $1 \leq i \leq n$
$k = 2$
while $k \leq n$ do
    for $j = (k-1)$ downto 1 do — Perform size reduction
        Let $q_j = \lfloor \mu_{k,j} \rceil$ and set $b_k = b_k - q_j b_j$
        Update the values $\mu_{k,j}$ for $1 \leq j < k$
    end for
    if $B_k \geq (\delta - \mu_{k,k-1}^2) B_{k-1}$ then — Check Lovász condition
        $k = k + 1$
    else
        Swap b_k with b_{k-1}
        Update the values $b_k^*, b_{k-1}^*, B_k, B_{k-1}, \mu_{k-1,j}$ and $\mu_{k,j}$ for $1 \leq j < k$, and $\mu_{i,k}, \mu_{i,k-1}$ for $k < i \leq n$
        $k = \max\{2, k-1\}$
    end if
end while

The following fact is easy to prove.

Proposition 2 *If the LLL algorithm terminates then the output basis is LLL reduced.*

So it is crucial to guarantee that LLL actually terminates, and it does so in polynomial time. The following theorem was proved by Lenstra, Lenstra and Lovász (note that it only guarantees a precise complexity bound for lattices in $\mathbb{Z}^m$).

Theorem 2 *Let* L *be a lattice in* $\mathbb{Z}^m$ *with basis* $b_1, \ldots, b_n$ *and let* $X \in \mathbb{Z}_{\geq 2}$ *be such that* $||b_i||^2 \leq X$ *for* $1 \leq i \leq n$. *Let* $1/4 < \delta < 1$. *Then the LLL algorithm with factor* δ *terminates and performs* $O(n^2 \log(X))$ *iterations.*

We can therefore conclude that an LLL reduced basis exists for every lattice.