Chapter 18

Algorithms for the Closest and Shortest Vector Problems

This chapter presents several algorithms to find lattice vectors close to a given vector. First we consider two methods due to Babai that, although not guaranteed to solve the closest vector problem, are useful in several situations in the book. Then we present an exponential-time algorithm to enumerate all vectors close to a given point. This algorithm can be used to solve the closest and shortest vector problems. We then briefly mention a lattice basis reduction algorithm that is guaranteed to yield better approximate solutions to the shortest vector problem.

The closest vector problem (CVP) was defined in Section 16.3. First, we remark that the shortest distance from a given vector $\underline{w} \in \mathbb{R}^n$ to a lattice vector $\underline{v} \in L$ can be quite large compared with the lengths of short vectors in the lattice.

Example 18.0.1. Consider the lattice in $\mathbb{R}^2$ with basis $(1, 0)$ and $(0, 1000)$. Then $\underline{w} = (0, 500)$ has distance 500 from the closest lattice point, despite the fact that the first successive minimum is 1.

Exercise 18.0.2. Let $L = \mathbb{Z}^n$ and $\underline{w} = (1/2, \dots, 1/2)$. Show that $\|\underline{w} - \underline{v}\| \geq \sqrt{n}/2$ for all $\underline{v} \in L$. Hence, show that if $n > 4$ then $\|\underline{w} - \underline{v}\| > \lambda_n$ for all $\underline{v} \in L$.

18.1 Babai's Nearest Plane Method

Let L be a full rank lattice given by an (ordered) basis $\{\underline{b}_1, \dots, \underline{b}_n\}$ and let $\{\underline{b}_1^*, \dots, \underline{b}_n^*\}$ be the corresponding Gram-Schmidt basis. Let $\underline{w} \in \mathbb{R}^n$. Babai [18] presented a method to inductively find a lattice vector close to $\underline{w}$. The vector $\underline{v} \in L$ output by Babai's method is not guaranteed to be such that $\|\underline{w} - \underline{v}\|$ is minimal. Theorem 18.1.6 shows that if the lattice basis is LLL-reduced then $\|\underline{w} - \underline{v}\|$ is within an exponential factor of the minimal value.

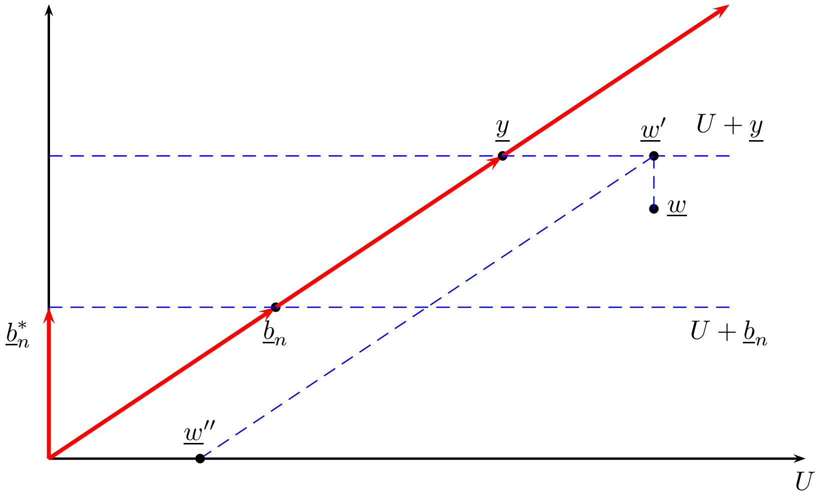

Figure 18.1: Illustration of the Babai nearest plane method. The x-axis represents the subspace U (which has dimension $n-1$) and the y-axis is perpendicular to U.

We now describe the method. Define $U = \operatorname{span}\{\underline{b}_1, \dots, \underline{b}_{n-1}\}$ and let $L' = L \cap U$ be the sublattice spanned by $\{\underline{b}_1, \dots, \underline{b}_{n-1}\}$. The idea of the nearest plane method is to find a vector $\underline{y} \in L$ such that the distance from $\underline{w}$ to the plane $U + \underline{y}$ is minimal. One then sets $\underline{w}'$ to be the orthogonal projection of $\underline{w}$ onto the plane $U + \underline{y}$ (in other words, $\underline{w}' \in U + \underline{y}$ and $\underline{w} - \underline{w}' \in U^\perp$). Let $\underline{w}'' = \underline{w}' - \underline{y} \in U$. Note that if $\underline{w} \notin L$ then $\underline{w}'' \notin L$. One inductively solves the (lower dimensional) closest vector problem of $\underline{w}''$ in L' to get $\underline{y}' \in L'$. The solution to the original instance of the CVP is $\underline{v} = \underline{y} + \underline{y}'$.

We now explain how to algebraically find $\underline{y}$ and $\underline{w}'$.

Lemma 18.1.1. *Let*

$$\underline{w} = \sum_{j=1}^{n} l_j \underline{b}_j^* \tag{18.1}$$

with $l_j \in \mathbb{R}$. Define $\underline{y} = \lfloor l_n \rceil \underline{b}_n \in L$ (where $\lfloor l_n \rceil$ denotes rounding to the nearest integer) and $\underline{w}' = \sum_{j=1}^{n-1} l_j \underline{b}_j^* + \lfloor l_n \rceil \underline{b}_n^*$. Then $\underline{y}$ is such that the distance between $\underline{w}$ and $U + \underline{y}$ is minimal, and $\underline{w}'$ is the orthogonal projection of $\underline{w}$ onto $U + \underline{y}$.

Proof: We use the fact that $U = \operatorname{span}\{\underline{b}_1^*, \dots, \underline{b}_{n-1}^*\}$. The distance from $\underline{w}$ to $U + \underline{y}$ is

$$\inf_{\underline{u} \in U} \|\underline{w} - (\underline{u} + \underline{y})\|.$$

Let $\underline{w}$ be as in equation (18.1) and let $\underline{y} = \sum_{j=1}^{n} l'_j \underline{b}_j$ be any element of L for $l'_j \in \mathbb{Z}$. One can write $\underline{y} = \sum_{j=1}^{n-1} l''_j \underline{b}_j^* + l'_n \underline{b}_n^*$ for some $l''_j \in \mathbb{R}$, $1 \le j \le n-1$.

Lemma A.10.5 shows that, for fixed $\underline{w}$ and $\underline{y}$, $\|\underline{w} - (\underline{u} + \underline{y})\|^2$ is minimised by $\underline{u} = \sum_{j=1}^{n-1} (l_j - l''_j) \underline{b}_j^* \in U$. Indeed,

$$\|\underline{w} - (\underline{u} + \underline{y})\|^2 = (l_n - l'_n)^2 \|\underline{b}_n^*\|^2.$$

It follows that one must take $l_n' = \lfloor l_n \rceil$, and so the choice of $\underline{y}$ in the statement of the Lemma is correct (note that one can add any element of L' to $\underline{y}$ and it is still a valid choice).

The vector $\underline{w}'$ satisfies

$$\underline{w}' - \underline{y} = \sum_{j=1}^{n-1} l_j \underline{b}_j^* + \lfloor l_n \rceil (\underline{b}_n^* - \underline{b}_n) \in U,$$

which shows that $\underline{w}' \in U + \underline{y}$. Also,

$$\underline{w} - \underline{w}' = \sum_{j=1}^{n} l_j \underline{b}_j^* - \sum_{j=1}^{n-1} l_j \underline{b}_j^* - \lfloor l_n \rceil \underline{b}_n^* = (l_n - \lfloor l_n \rceil)\underline{b}_n^*, \qquad (18.2)$$

which is orthogonal to U. Hence, $\underline{w}'$ is the orthogonal projection of $\underline{w}$ onto $U + \underline{y}$. □

Exercise 18.1.2. Let the notation be as above and write $\underline{b}_n = \underline{b}_n^* + \sum_{i=1}^{n-1} \mu_{n,i} \underline{b}_i^*$. Show that

$$\underline{w}'' = \sum_{i=1}^{n-1} (l_i - \lfloor l_n \rceil \mu_{n,i}) \underline{b}_i^*.$$

Exercise 18.1.3. Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be an ordered basis for a lattice L. Let $\underline{w} \in \mathbb{R}^n$ and suppose that there is an element $\underline{v} \in L$ such that $\|\underline{v} - \underline{w}\| < \frac{1}{2}\|\underline{b}_i^*\|$ for all $1 \le i \le n$. Prove that the nearest plane algorithm outputs $\underline{v}$.

The following Lemma is needed to prove the main result, namely Theorem 18.1.6.

Lemma 18.1.4. *Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be LLL reduced (with respect to the Euclidean norm, and with factor $\delta = 3/4$). If $\underline{v}$ is the output of Babai's nearest plane algorithm on input $\underline{w}$ then*

$$\|\underline{w} - \underline{v}\|^2 \le \tfrac{2^n - 1}{4} \|\underline{b}_n^*\|^2.$$

Proof: We prove the result by induction. Certainly if $n = 1$ then $\|\underline{w} - \underline{v}\|^2 \le \frac{1}{4}\|\underline{b}_1^*\|^2$ as required.

Now suppose $n \ge 2$. Recall that the output of the method is $\underline{v} = \underline{y} + \underline{y}'$ where $\underline{y} \in L$ minimises the distance from $\underline{w}$ to $U + \underline{y}$, $\underline{w}'$ is the orthogonal projection of $\underline{w}$ onto $U + \underline{y}$, and $\underline{y}'$ is the output of the algorithm on $\underline{w}'' = \underline{w}' - \underline{y}$ in L'. By the inductive hypothesis we know that $\|\underline{w}'' - \underline{y}'\|^2 \le \frac{1}{4}(2^{n-1} - 1)\|\underline{b}_{n-1}^*\|^2$. Hence

$$\begin{aligned} \|\underline{w} - (\underline{y} + \underline{y}')\|^2 &= \|\underline{w} - \underline{w}' + \underline{w}' - (\underline{y} + \underline{y}')\|^2 \\ &= \|\underline{w} - \underline{w}'\|^2 + \|\underline{w}'' - \underline{y}'\|^2 \\ &\le \tfrac{1}{4}\|\underline{b}_n^*\|^2 + \tfrac{2^{n-1}-1}{4}\|\underline{b}_{n-1}^*\|^2 \end{aligned}$$

using equation (18.2).

Finally, part 1 of Lemma 17.2.8 implies that this is

$$\le \left(\tfrac{1}{4} + 2\tfrac{2^{n-1}-1}{4} \right) \|\underline{b}_n^*\|^2$$

from which the result follows. □

Exercise 18.1.5. Prove that if $\underline{v}$ is the output of the nearest plane algorithm on input $\underline{w}$ then

$$\|\underline{v} - \underline{w}\|^2 \le \tfrac{1}{4} \sum_{i=1}^{n} \|\underline{b}_i^*\|^2.$$

Theorem 18.1.6. *If the basis $\{\underline{b}_1, \dots, \underline{b}_n\}$ is LLL-reduced (with respect to the Euclidean norm and with factor $\delta = 3/4$) then the output of the Babai nearest plane algorithm on $\underline{w} \in \mathbb{R}^n$ is a vector $\underline{v}$ such that $\|\underline{v} - \underline{w}\| < 2^{n/2}\|\underline{u} - \underline{w}\|$ for all $\underline{u} \in L$.*

Proof: We prove the result by induction. For $n = 1$, $\underline{v}$ is a correct solution to the closest vector problem and so the result holds.

Let $n \geq 2$ and let $\underline{u} \in L$ be a closest vector to $\underline{w}$. Let $\underline{y}$ be the vector chosen in the first step of the Babai method. We consider two cases.

1. Case $\underline{u} \in U + \underline{y}$. Then $\|\underline{u} - \underline{w}\|^2 = \|\underline{u} - \underline{w}'\|^2 + \|\underline{w}' - \underline{w}\|^2$ so $\underline{u}$ is also a closest vector to $\underline{w}'$. Hence $\underline{u} - \underline{y}$ is a closest vector to $\underline{w}'' = \underline{w}' - \underline{y} \in U$. Let $\underline{y}'$ be the output of the Babai nearest plane algorithm on $\underline{w}''$. By the inductive hypothesis,
$$\|\underline{y}' - \underline{w}''\| < 2^{(n-1)/2}\|\underline{u} - \underline{y} - \underline{w}''\|.$$
Substituting $\underline{w}' - \underline{y}$ for $\underline{w}''$ gives
$$\|\underline{y} + \underline{y}' - \underline{w}'\| < 2^{(n-1)/2}\|\underline{u} - \underline{w}'\|.$$
Now
$$\|\underline{v} - \underline{w}\|^2 = \|\underline{y} + \underline{y}' - \underline{w}'\|^2 + \|\underline{w}' - \underline{w}\|^2 < 2^{n-1}\|\underline{u} - \underline{w}'\|^2 + \|\underline{w}' - \underline{w}\|^2.$$
Using $\|\underline{u} - \underline{w}'\|, \|\underline{w}' - \underline{w}\| \leq \|\underline{u} - \underline{w}\|$ and $2^{n-1} + 1 \leq 2^n$ gives the result.

2. Case $\underline{u} \notin U + \underline{y}$. Since the distance from $\underline{w}$ to $U + \underline{y}$ is $\leq \frac{1}{2}\|\underline{b}_n^*\|$, we have $\|\underline{w} - \underline{u}\| \geq \frac{1}{2}\|\underline{b}_n^*\|$. By Lemma 18.1.4 we find
$$\tfrac{1}{2}\|\underline{b}_n^*\| \geq \tfrac{1}{2}\sqrt{\frac{4}{2^n - 1}}\|\underline{w} - \underline{v}\|.$$
Hence, $\|\underline{w} - \underline{v}\| < 2^{n/2}\|\underline{w} - \underline{u}\|$.

This completes the proof. □

One can obtain a better result by using the result of Lemma 17.2.9.

Theorem 18.1.7. *If the basis $\{\underline{b}_1, \dots, \underline{b}_n\}$ is LLL-reduced with respect to the Euclidean norm and with factor $\delta = 1/4 + 1/\sqrt{2}$ then the output of the Babai nearest plane algorithm on $\underline{w} \in \mathbb{R}^n$ is a vector $\underline{v}$ such that*
$$\|\underline{v} - \underline{w}\| < \frac{2^{n/4}}{\sqrt{\sqrt{2} - 1}}\|\underline{u} - \underline{w}\| < (1.6)2^{n/4}\|\underline{u} - \underline{w}\|$$
for all $\underline{u} \in L$.

Exercise 18.1.8. Prove Theorem 18.1.7.
[Hint: First prove that the analogue of Lemma 18.1.4 in this case is $\|\underline{w} - \underline{v}\|^2 \leq (2^{n/2} - 1)/(4(\sqrt{2} - 1))\|\underline{b}_n^*\|^2$. Then follow the proof of Theorem 18.1.6 using the fact that $\left(2^{(n-1)/4}/\sqrt{\sqrt{2} - 1}\right)^2 + 1 \leq \left(2^{n/4}/\sqrt{\sqrt{2} - 1}\right)^2$.]

Algorithm 26 is the Babai nearest plane algorithm. We use the notation $\underline{y}_n = \underline{y}$, $\underline{w}_n = \underline{w}$, $\underline{w}_{n-1} = \underline{w}''$ etc. Note that Babai's algorithm can be performed using exact arithmetic over $\mathbb{Q}$ or using floating point arithmetic.

Algorithm 26 Babai nearest plane algorithm

```
INPUT: $\{\underline{b}_1, \ldots, \underline{b}_n\}, \underline{w}$
OUTPUT: $\underline{v}$
  Compute Gram-Schmidt basis $\underline{b}_1^*, \ldots, \underline{b}_n^*$
  Set $\underline{w}_n = \underline{w}$
  for $i = n$ downto 1 do
      Compute $l_i = \langle \underline{w}_i, \underline{b}_i^* \rangle / \langle \underline{b}_i^*, \underline{b}_i^* \rangle$
      Set $\underline{y}_i = \lfloor l_i \rceil \underline{b}_i$
      Set $\underline{w}_{i-1} = \underline{w}_i - (l_i - \lfloor l_i \rceil)\underline{b}_i^* - \lfloor l_i \rceil \underline{b}_i$
  end for
  return $\underline{v} = \underline{y}_1 + \cdots + \underline{y}_n$
```

Exercise 18.1.9. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be a basis for a lattice in $\mathbb{Z}^n$. Let $X \in \mathbb{R}_{>0}$ be such that $\|\underline{b}_i\| \leq X$ for $1 \leq i \leq n$. Show that the complexity of the Babai nearest plane algorithm (not counting LLL) when using exact arithmetic over $\mathbb{Q}$ is $O(n^5 \log(X)^2)$ bit operations.

Exercise 18.1.10. If $\{\underline{b}_1, \ldots, \underline{b}_n\}$ is an ordered LLL-reduced basis then $\underline{b}_1$ is likely to be shorter than $\underline{b}_n$. It would therefore be more natural to start with $\underline{b}_1$ and define U to be the orthogonal complement of $\underline{b}_1$. Why is this not possible?

Example 18.1.11. Consider the LLL-reduced basis

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 0 & -3 \\ 3 & -7 & 3 \end{pmatrix}$$

and the vector $\underline{w} = (10, 6, 5) \in \mathbb{R}^3$. We perform the nearest plane method to find a lattice vector close to $\underline{w}$.

First compute the Gram-Schmidt basis $\underline{b}_1^* = (1, 2, 3)$, $\underline{b}_2^* = (24/7, 6/7, -12/7)$ and $\underline{b}_3^* = (10/3, -20/3, 10/3)$. Write

$$\underline{w} = \tfrac{37}{14}\underline{b}_1^* + 2\underline{b}_2^* + \tfrac{3}{20}\underline{b}_3^*.$$

Since $\lfloor 3/20 \rceil = 0$ we have $\underline{y}_3 = 0$ and $\underline{w}'' = \underline{w}' = \frac{37}{14}\underline{b}_1^* + 2\underline{b}_2^* = (19/2, 7, 9/2)$. The process is continued inductively, so write $\underline{w} = \underline{w}''$. Then one takes $\underline{y}_2 = 2\underline{b}_2 = (6, 0, -6)$ and $\underline{w}'' = \underline{w} - \underline{y}_2 = (7/2, 7, 21/2) = \frac{7}{2}\underline{b}_1^*$. Since $\lfloor 7/2 \rceil = 3$ we return the solution

$$3\underline{b}_1 + 2\underline{b}_2 = (9, 6, 3).$$

Exercise 18.1.12. Show that the vector $\underline{v}$ output by the Babai nearest plane method lies in the parallelepiped

$$\left\{ \underline{w} + \sum_{j=1}^{n} l_j \underline{b}_j^* : l_j \in \mathbb{R}, |l_j| \leq \tfrac{1}{2} \right\}$$

centered on $\underline{w}$. Show that this parallelepiped has volume equal to the volume of the lattice. Hence show that if $\underline{w}$ does not lie in the lattice then there is exactly one lattice point in this parallelepiped.

Show that if there exists a vector $\underline{v} \in L$ such that $\|\underline{v} - \underline{w}\| \leq \frac{1}{2}\min\{\|\underline{b}_i^*\| : 1 \leq i \leq n\}$ then the Babai nearest plane algorithm on input $\underline{w}$ outputs $\underline{v}$.

Some improvements to the Babai nearest plane algorithm are listed in Section 3.4 of [256] (where they are credited to Coppersmith). Similar methods (but using a randomised choice of plane) were used by Klein [341] to solve the CVP when the target vector is particularly close to a lattice point. Another variant of the nearest plane algorithm is given by Lindner and Peikert [390]. The nearest plane algorithm is known by the name "VBLAST" in the communications community (see [440]).

18.2 Babai's Rounding Technique

An alternative to the nearest plane method is the rounding technique. This is simpler to compute in practice, since it does not require the computation of a Gram-Schmidt basis, but harder to analyse in theory. This method is also not guaranteed to solve CVP. Let $\underline{b}_1, \dots, \underline{b}_n$ be a basis for a full rank lattice in $\mathbb{R}^n$. Given a target $\underline{w} \in \mathbb{R}^n$ we can write

$$\underline{w} = \sum_{i=1}^{n} l_i \underline{b}_i$$

with $l_i \in \mathbb{R}$. One computes the coefficients l_i by solving the system of linear equations (since the lattice is full rank we can also compute the vector $(l_1, \dots, l_n)$ as $\underline{w}B^{-1}$). The rounding technique is simply to set

$$\underline{v} = \sum_{i=1}^{n} \lfloor l_i \rceil \underline{b}_i$$

where $\lfloor l \rceil$ means take the closest integer to the real number l. This procedure can be performed using any basis for the lattice. Babai has proved that $\|\underline{v} - \underline{w}\|$ is within an exponential factor of the minimal value if the basis is LLL-reduced. The method trivially generalises to non-full-rank lattices as long as $\underline{w}$ lies in the $\mathbb{R}$-span of the basis.

Theorem 18.2.1. *Let $\underline{b}_1, \dots, \underline{b}_n$ be an LLL-reduced basis (with respect to the Euclidean norm and with factor $\delta = 3/4$) for a lattice $L \subseteq \mathbb{R}^n$. Then the output $\underline{v}$ of the Babai rounding method on input $\underline{w} \in \mathbb{R}^n$ satisfies*

$$\|\underline{w} - \underline{v}\| \le (1 + 2n(9/2)^{n/2})\|\underline{w} - \underline{u}\|$$

for all $\underline{u} \in L$.

Proof: See Babai [18]. □

Babai rounding gives a lattice point $\underline{v}$ such that $\underline{w} - \underline{v} = \sum_{i=1}^{n} m_i \underline{b}_i$ where $|m_i| \le 1/2$. In other words, $\underline{v}$ lies in the parallelepiped, centered at $\underline{w}$, defined by the basis vectors. Since the volume of the parallelepiped is equal to the volume of the lattice, if $\underline{w}$ is not in the lattice then there is exactly one lattice point in the parallelepiped. The geometry of the parallelepiped determines whether or not an optimal solution to the CVP is found. Hence, though the rounding method can be used with any basis for a lattice, the result depends on the quality of the basis.

Example 18.2.2. Let $\underline{b}_1 = (3, 2)$ and $\underline{b}_2 = (2, 1)$ generate the lattice $\mathbb{Z}^2$. Let $\underline{w} = (-0.4, 0.4)$ so that the solution to CVP is $(0, 0)$. One can verify that $(-0.4, 0.4) = 1.2\underline{b}_1 - 2\underline{b}_2$ and so Babai rounding yields $\underline{b}_1 - 2\underline{b}_2 = (-1, 0)$. Figure 18.2 shows the parallelepiped centered at $\underline{w}$ corresponding to the basis. One can see that $(-1, 0)$ is the only lattice point within that parallelepiped.

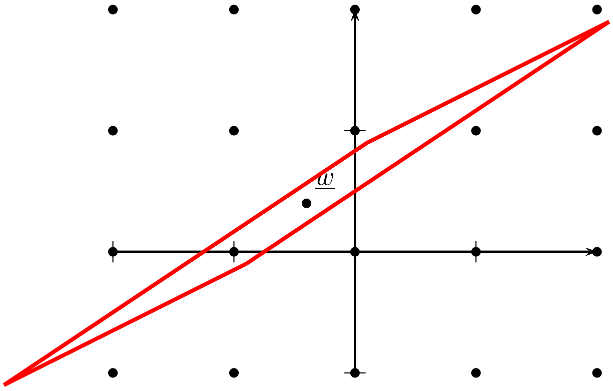

Figure 18.2: Parallelepiped centered at $(-0.4, 0.4)$ corresponding to lattice basis $(3, 2)$ and $(2, 1)$.

Exercise 18.2.3. Consider the vector $\underline{w} = (-0.4, 0.4)$ as in Example 18.2.2 again. Using the basis $\{(1, 0), (0, 1)\}$ for $\mathbb{Z}^2$ use the Babai rounding method to find the closest lattice vector in $\mathbb{Z}^2$ to $\underline{w}$. Draw the parallelepiped centered on $\underline{w}$ in this case.

We stress that the rounding method is not the same as the nearest plane method. The next example shows that the two methods can give different results.

Example 18.2.4. Consider the CVP instance in Example 18.1.11. We have

$$\underline{w} = \tfrac{141}{40}\underline{b}_1 + \tfrac{241}{120}\underline{b}_2 + \tfrac{3}{20}\underline{b}_3.$$

Hence one sets

$$\underline{v} = 4\underline{b}_1 + 2\underline{b}_2 = (10, 8, 6) \neq (9, 6, 3).$$

Note that this is a different solution to the one found in Example 18.1.11, though both solutions satisfy $\|\underline{w} - \underline{v}\| = \sqrt{5}$.

Exercise 18.2.5. Prove that if $\underline{b}_1, \dots, \underline{b}_n$ are orthogonal basis vectors for a lattice L then the Babai rounding technique produces a correct solution to the CVP with respect to the Euclidean norm. Show also that the Babai rounding technique gives the same result as the Babai nearest plane method in this case.

Exercise 18.2.6. Show that the nearest plane and rounding methods produce a linear combination of the lattice basis where the vector $\underline{b}_n$ has the same coefficient.

Exercise 18.2.7. Consider the lattice with basis

$$\begin{pmatrix} 7 & 0 & 1 \\ 1 & 17 & 1 \\ -3 & 0 & 10 \end{pmatrix}$$

and let

$$\underline{w} = (100, 205, 305).$$

Find a lattice vector $\underline{v}$ close to $\underline{w}$ using the rounding technique. What is $\|\underline{v} - \underline{w}\|$?

The Babai rounding algorithm is known by the name "zero forcing" in the communications community (see [440]).

18.3 The Embedding Technique

Another way to solve CVP is the **embedding technique**, due to Kannan (see page 437 onwards of [330]). Let B be a basis matrix for a lattice L and suppose $\underline{w} \in \mathbb{R}^n$ (in practice we assume $\underline{w} \in \mathbb{Q}^n$). A solution to the CVP corresponds to integers $l_1, \dots, l_n$ such that

$$\underline{w} \approx \sum_{i=1}^{n} l_i \underline{b}_i.$$

The crucial observation is that $\underline{e} = \underline{w} - \sum_{i=1}^n l_i \underline{b}_i$ is such that $\|\underline{e}\|$ is small.

The idea of the embedding technique is to define a lattice L' that contains the short vector $\underline{e}$. Let $M \in \mathbb{R}_{>0}$ (for example $M = 1$). The lattice L' is defined by the vectors (which are a basis for $\mathbb{R}^{n+1}$)

$$(\underline{b}_1, 0),\ \cdots,\ (\underline{b}_n, 0),\ (\underline{w}, M). \tag{18.3}$$

One sees that taking the linear combination of rows with coefficients $(-l_1, \dots, -l_n, 1)$ gives the vector

$$(\underline{e}, M).$$

Hence, we might be able to find $\underline{e}$ by solving the SVP problem in the lattice L'. One can then solve the CVP by subtracting $\underline{e}$ from $\underline{w}$.

Example 18.3.1. Consider the basis matrix

$$B = \begin{pmatrix} 35 & 72 & -100 \\ -10 & 0 & -25 \\ -20 & -279 & 678 \end{pmatrix}$$

for a lattice in $\mathbb{R}^3$. We solve the CVP instance with $\underline{w} = (100, 100, 100)$.

Apply the LLL algorithm to the basis matrix (taking $M = 1$)

$$\begin{pmatrix} 35 & 72 & -100 & 0 \\ -10 & 0 & -25 & 0 \\ -20 & -279 & 678 & 0 \\ 100 & 100 & 100 & 1 \end{pmatrix}$$

for the lattice L'. This gives the basis matrix

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 5 & 0 & 1 & 0 \\ 0 & 5 & 1 & -4 \\ 5 & 5 & -21 & -4 \end{pmatrix}.$$

The first row is $(0, 1, 0, 1)$, so we know that $(0, 1, 0)$ is the difference between $\underline{w}$ and a lattice point $\underline{v}$. One verifies that $\underline{v} = (100, 100, 100) - (0, 1, 0) = (100, 99, 100)$ is a lattice point.

The success of the embedding technique depends on the size of $\underline{e}$ compared with the lengths of short vectors in the original lattice L. As we have seen in Exercise 18.0.2, $\underline{e}$ can be larger than λ_n, in which case the embedding technique is not likely to be a good way to solve the closest vector problem.

Lemma 18.3.2. *Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be a basis for a lattice $L \subseteq \mathbb{Z}^n$ and denote by λ_1 the shortest Euclidean length of a non-zero element of L. Let $\underline{w} \in \mathbb{R}^n$ and let $\underline{v} \in L$ be a closest lattice point to $\underline{w}$. Define $\underline{e} = \underline{w} - \underline{v}$. Suppose that $\|\underline{e}\| < \lambda_1/2$ and let $M = \|\underline{e}\|$. Then $(\underline{e}, M)$ is a shortest non-zero vector in the lattice L' of the embedding technique.*

Proof: All vectors in the lattice L' are of the form

$$l_{n+1}(\underline{e}, M) + \sum_{i=1}^{n} l_i(\underline{b}_i, 0)$$

for some $l_1, \dots, l_{n+1} \in \mathbb{Z}$. Every non-zero vector with $l_{n+1} = 0$ is of length at least λ_1. Since

$$\|(\underline{e}, M)\|^2 = \|\underline{e}\|^2 + M^2 = 2M^2 < 2\lambda_1^2/4$$

the vector $(\underline{e}, \pm M)$ has length at most $\lambda_1/\sqrt{2}$. Since $\underline{v}$ is a closest vector to $\underline{w}$ it follows that $\|\underline{e}\| \le \|\underline{e} + \underline{x}\|$ for all $\underline{x} \in L$ and so every other vector $(\underline{u}, M) \in L'$ has length at least as large. Finally, suppose $|l_{n+1}| \ge 2$. Then

$$\|(\underline{u}, l_{n+1}M)\|^2 \ge \|(0, l_{n+1}M)\|^2 \ge (2M)^2$$

and so $\|(\underline{u}, l_{n+1}M)\| \ge 2\|(\underline{e}, M)\|$. □

Lemma 18.3.2 shows that the CVP can be reduced to SVP as long as the target vector is very close to a lattice vector, and assuming one has a good guess M for the distance. However, when using algorithms such as LLL that solve the approximate SVP it is not possible, in general, to make rigorous statements about the success of the embedding technique. As mentioned earlier, the LLL algorithm often works better than the theoretical analysis predicts. Hence the embedding technique can potentially be useful even when $\underline{w}$ is not so close to a lattice point. For further discussion see Lemma 6.15 of Kannan [330].

Exercise 18.3.3. Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be a basis for a lattice in $\mathbb{R}^n$ and let $\underline{w} \in \mathbb{R}^n$. Let $M = \max_{1 \le i \le n} \|\underline{b}_i\|$. Show that the output $(\underline{e}, M)$ of the embedding technique (using LLL) on the basis of equation (18.3) is the same as the output of the Babai nearest plane algorithm when run on the LLL-reduced basis.

Exercise 18.3.4. Solve the following CVP instance using the embedding technique and a computer algebra package.

$$B = \begin{pmatrix} -265 & 287 & 56 \\ -460 & 448 & 72 \\ -50 & 49 & 8 \end{pmatrix}, \qquad \underline{w} = (100, 80, 100).$$

18.4 Enumerating all Short Vectors

We present a method to enumerate all short vectors in a lattice, given any basis. We will show later that the performance of this enumeration algorithm depends on the quality of the lattice basis. Throughout this section, $\|\underline{v}\|$ denotes the Euclidean norm.

The first enumeration method was given by Pohst in 1981. Further variants were given by Finke and Pohst, Kannan [329, 330], Helfrich [281] and Schnorr and Euchner [526]. These methods are all deterministic and are guaranteed to output a non-zero vector of minimum length. The time complexity is exponential in the lattice dimension, but the storage requirements are polynomial. This approach is known by the name “sphere decoding” in the communications community (see [440]).

Exercise 18.4.1. Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an (ordered) basis in $\mathbb{R}^m$ for a lattice and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation. Let $\underline{v} \in \mathbb{R}^m$. Show that the projection of $\underline{v}$ onto $\underline{b}_i^*$ is

$$\frac{\langle \underline{v}, \underline{b}_i^* \rangle}{\|\underline{b}_i^*\|^2} \underline{b}_i^*.$$

Show that if $\underline{v} = \sum_{j=1}^n x_j \underline{b}_j$ then this projection is

$$\left(x_i + \sum_{j=i+1}^n x_j \mu_{j,i} \right) \underline{b}_i^*.$$

Lemma 18.4.2. *Let $\{\underline{b}_1, \ldots, \underline{b}_n\}$ be an (ordered) basis for a lattice and let $\{\underline{b}_1^*, \ldots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation. Fix $A \in \mathbb{R}_{>0}$ and write $B_i = \|\underline{b}_i^*\|^2$. Let $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i$ be such that $\|\underline{v}\|^2 \le A$. For $1 \le i \le n$ define*

$$z_i = x_i + \sum_{j=i+1}^n \mu_{j,i} x_j.$$

Then for $1 \le i < n$

$$\sum_{i=1}^n z_i^2 B_i \le A.$$

Proof: Exercise 18.4.1 gives a formula $z_i \underline{b}_i^*$ for the projection of $\underline{v}$ onto each $\underline{b}_i^*$. Since the vectors $\underline{b}_i^*$ are orthogonal we have

$$\|\underline{v}\|^2 = \sum_{i=1}^n \|z_i \underline{b}_i^*\|^2 = \sum_{i=1}^n z_i^2 B_i.$$

The result follows. □

Theorem 18.4.3. *Let the notation be as in Lemma 18.4.2. Then one has $x_n^2 \le A/\|\underline{b}_n^*\|^2$ and, for $1 \le i < n$,*

$$\left(x_i + \sum_{j=i+1}^n \mu_{j,i} x_j \right)^2 B_i \le A - \sum_{j=i+1}^n z_j^2 B_j.$$

Proof: Note that $z_n = x_n$ and Lemma 18.4.2 implies $z_n^2 B_n \le A$, which proves the first statement. The second statement is also just a re-writing of Lemma 18.4.2. □

We now sketch the enumeration algorithm for finding all short lattice vectors $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i$, which follows from the above results. First, without loss of generality we may assume that $x_n \ge 0$. By Theorem 18.4.3 we know $0 \le x_n \le \sqrt{A/B_n}$. For each candidate x_n one knows that

$$(x_{n-1} + \mu_{n,n-1} x_n)^2 B_{n-1} \le A - x_n^2 B_n$$

and so

$$|x_{n-1} + \mu_{n,n-1} x_n| \le \sqrt{(A - x_n^2 B_n)/B_{n-1}}.$$

To phrase this as a bound on x_{n-1} one uses the fact that for any $a \in \mathbb{R}, b \in \mathbb{R}_{\ge 0}$, the solutions $x \in \mathbb{R}$ to $|x + a| \le b$ satisfy $-(b + a) \le x \le b - a$. Hence, writing $M_1 = \sqrt{(A - x_n^2 B_n)/B_{n-1}}$ one has

$$-(M_1 + \mu_{n,n-1} x_n) \le x_{n-1} \le M_1 - \mu_{n,n-1} x_n.$$

Exercise 18.4.4. Generalise the above discussion to show that for $1 \le i < n$ one has

$$-(M_1 + M_2) \le x_i \le M_1 - M_2$$

where

$$M_1 = \sqrt{\left(A - \sum_{j=i+1}^{n} x_j^2 B_j \right) / B_i}$$

and $M_2 = \sum_{j=i+1}^{n} \mu_{j,i} x_j$.

Exercise 18.4.5. Write pseudocode for the algorithm to enumerate all short vectors of a lattice.

The algorithm to find a non-zero vector of minimal length is then straightforward. Set A to be $\|\underline{b}_1\|^2$, enumerate all vectors of length at most A and, for each vector, compute the length. One is guaranteed to find a shortest vector in the lattice. Schnorr and Euchner [526] organised the search in a manner to minimise the running time.

The running time of this algorithm depends on the quality of the basis in several ways. First, it is evidently important to have a good bound A for the length of the shortest vector. Taking $A = \|\underline{b}_1\|^2$ is only sensible if $\underline{b}_1$ is already rather short; alternatively one may choose, say, $A = \sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}$ using the Gaussian heuristic (one can choose a small bound for A and then, if the search fails, increase A accordingly). Second, one sees that if $\underline{b}_n^*$ is very short then the algorithm searches a huge range of values for x_n, and similarly if $\underline{b}_{n-1}^*$ is very short etc. Hence, the algorithm performs best if the values $\|\underline{b}_i^*\|$ descrease rather gently.

To solve SVP in practice using enumeration one first performs LLL and other precomputation to get a sufficiently nice basis. We refer to Kannan [329, 330], Schnorr and Euchner [526] and Agrell et al [7] for details. The best complexity statement in the literature is due to Hanrot and Stehlé.

Theorem 18.4.6. *(Hanrot and Stehlé [275]) There exists a polynomial $p(x, y) \in \mathbb{R}[x, y]$ such that, for any n-dimensional lattice L in $\mathbb{Z}^m$ with basis consisting of vectors with coefficients bounded by B, one can compute all the shortest non-zero vectors in L in at most $p(\log(B), m)n^{n/2e+o(n)}$ bit operations.*

Exercise 18.4.7. Let L be a lattice in $\mathbb{Z}^n$ that contains $q\mathbb{Z}^n$ for some integer q. Let $M \in \mathbb{N}$ be a fixed bound. Give an algorithm based on Wagner's technique (see Section 13.8) for finding vectors in L with all entries bounded by M. Determine the complexity of this algorithm.

Due to lack of space we refer to the original papers for further details about enumeration algorithms. Pujol and Stehlé [491] give an analysis of issues related to floating point implementation.

In practice the most efficient enumeration methods for the SVP are heuristic "pruning" methods. These methods are still exponential in the lattice dimension, and are not guaranteed to output the shortest vector. The extreme pruning algorithm of Gama, Nguyen and Regev [235] is currently the most practical method.

A quite different approach, leading to non-deterministic algorithms (in other words, the output is a non-zero vector in the lattice that, with high probability, has minimal length) is due to Ajtai, Kumar and Sivakumar (see [357] for a survey). The running time and storage requirements of the algorithm are both exponential in the lattice dimension. For some experimental results we refer to Nguyen and Vidick [465]. Micciancio and Voulgaris [424] have given an improved algorithm, still requiring exponential time and storage.

18.4.1 Enumeration of Closest Vectors

The above ideas can be adapted to list lattice points close to some $\underline{w} \in \mathbb{R}^n$. Let $A \in \mathbb{R}_{>0}$ and suppose we seek all $\underline{v} \in L$ such that $\|\underline{v} - \underline{w}\|^2 \le A$. Write $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i = \sum_{i=1}^n z_i \underline{b}_i^*$ as before and write

$$\underline{w} = \sum_{i=1}^n y_i \underline{b}_i^*.$$

Then $\|\underline{v} - \underline{w}\|^2 \le A$ is equivalent to

$$\sum_{i=1}^n (z_i - y_i)^2 \|\underline{b}_i^*\|^2 \le A.$$

It follows that

$$y_n - \sqrt{A/B_n} \le x_n \le y_n + \sqrt{A/B_n}$$

and so on.

Lemma 18.4.8. *Let the notation be as above and define*

$$M_i = \sqrt{\left(A - \sum_{j=i+1}^n (z_j - y_j)^2 B_j \right) / B_i} \quad \text{and} \quad N_i = \sum_{j=i+1}^n \mu_{j,i} x_j$$

for $1 \le i \le n$. If $\underline{v} = \sum_{i=1}^n x_i \underline{b}_i$ satisfies $\|\underline{v} - \underline{w}\|^2 \le A$ then, for $1 \le i \le n$,

$$y_i - M_i - N_i \le x_i \le y_i + M_i - N_i$$

Exercise 18.4.9. Prove Lemma 18.4.8.

The paper by Agrell, Eriksson, Vardy and Zeger [7] gives an excellent survey and comparison of the various enumeration techniques. They conclude that the Schnorr-Euchner variant is much more efficient than the Pohst or Kannan versions.

18.5 Korkine-Zolotarev Bases

We present a notion of reduced lattice basis that has better properties than an LLL-reduced basis.

Definition 18.5.1. Let L be a lattice of rank n in $\mathbb{R}^m$. An ordered basis $\{\underline{b}_1, \dots, \underline{b}_n\}$ for L is **Korkine-Zolotarev reduced**[1] if

1. $\underline{b}_1$ is a non-zero vector of minimal length in L;
2. $|\mu_{i,1}| < 1/2$ for $2 \le i \le n$;
3. the basis $\{\underline{b}_2 - \mu_{2,1}\underline{b}_1, \dots, \underline{b}_n - \mu_{n,1}\underline{b}_1\}$ is Korkine-Zolotarev reduced (this is the orthogonal projection of the basis of L onto the orthogonal complement of $\underline{b}_1$)

where $\underline{b}_i^*$ is the Gram-Schmidt orthogonalisation and $\mu_{i,j} = \langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$.

One problem is that there is no known polynomial-time algorithm to compute a Korkine-Zolotarev basis.

[1] Some authors also call it Hermite-Korkine-Zolotarev (HKV) reduced.

Theorem 18.5.2. *Let* $\{\underline{b}_1, \dots, \underline{b}_n\}$ *be a Korkine-Zolotarev reduced basis of a lattice* L*. Then*

1. *for* $1 \le i \le n$,
$$\frac{4}{i+3}\lambda_i^2 \le \|\underline{b}_i\|^2 \le \frac{i+3}{4}\lambda_i^2;$$

2.
$$\prod_{i=1}^{n} \|\underline{b}_i\|^2 \le \left(\gamma_n^n \prod_{i=1}^{n} \frac{i+3}{4} \right) \det(L)^2.$$

Proof: See Theorem 2.1 and 2.3 of Lagarias, Lenstra and Schnorr [361]. □

As we have seen, for lattices of relatively small dimension it is practical to enumerate all short vectors. Hence one can compute a Korkine-Zolotarev basis for lattices of small dimension. Schnorr has developed the **block Korkine-Zolotarev** lattice basis reduction algorithm, which computes a Korkine-Zolotarev basis for small dimensional projections of the original lattice and combines this with the LLL algorithm. The output basis can be proved to be of a better quality than an LLL-reduced basis. This is the most powerful algorithm for finding short vectors in lattices of large dimension. Due to lack of space we are unable to present this algorithm; we refer to Schnorr [521] for details.