Scribe Notes for *Algorithmic Number Theory*
Class 22—June 17, 1998

Scribes: Nick Loehr, Lynn W. Jones, and Hussein Suleman

Abstract

We began discussion on Lattice Basis Reduction. First, we reviewed select topics in lattices and linear algebra. Then we went on to discuss the 60° Algorithm for reducing lattice bases in 2 dimensions. Finally, we calculated bounds for the length of a *short* vector in both the 2-dimensional and the generalized n-dimensional lattice reduction.

1 Introduction to Lattices

Definition 1.1. Let $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_m} \in \mathbb{R}^n$ be linearly independent vectors. Then the set

$$L = \left\{ \sum_{i=1}^{m} c_i \mathbf{b_i} : c_i \in \mathbb{Z} \right\}$$

is a *lattice* and $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_m}\}$ is a *basis* for the lattice.

Note that the coefficients c_i are integers but the components of the vectors $\mathbf{b_i}$ are not necessarily integers.

We can form a matrix from the elements of the basis as follows:

$$B = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_m} \end{pmatrix}.$$

We usually assume that $m = n$, so that B will be a square matrix. Every lattice has at least one basis and, in fact, has at least 2, except in the trivial case. When there is more than one basis, we can easily transform one basis into another using elementary row operations.

Proposition 1.2. *Let B be a matrix formed from the basis of a lattice, as indicated above. Let B' be the result of any number of elementary row operations applied to B. Then there is a matrix U such that $B' = UB$ and* $\det U \in \{-1, 1\}$. *Furthermore, any basis for L can be obtained this way.*

Proof. We prove only the last statement. Assume that $m = n$. Suppose $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ and $\{\mathbf{b'_1}, \mathbf{b'_2}, \ldots, \mathbf{b'_n}\}$ are both bases for L. Let $\mathbf{b_i} = (b_{i1}, b_{i2}, \ldots, b_{n1})$ and $\mathbf{b'_i} = (b'_{i1}, b'_{i2}, \ldots, b'_{n1})$. Let

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

and

$$B' = \begin{pmatrix} b'_{11} & \cdots & b'_{1n} \\ \vdots & & \vdots \\ b'_{n1} & \cdots & b'_{nn} \end{pmatrix}.$$

Each $\mathbf{b'_i}$ is an integer linear combination of the $\mathbf{b_i}$'s and we can express this as $b'_{ij} = \sum_{k=1}^{n} u_{ik} b_{kj}$.

Let

$$U = \begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \cdots & u_{nn} \end{pmatrix}.$$

Then we get $B' = UB$. Similarly we get $B = U'B'$ for some integer matrix U'. Therefore, $U^{-1} = U'$, and $\det U = 1/\det U'$. But $\det U, \det U' \in \mathbb{Z}$. Therefore, $\det U \in \{-1, 1\}$ i.e., $\det U$ must be a unit in $\mathbb{Z}$.

□

In addition to the above results, we can conclude that $|\det B| = |\det B'|$.

Definition 1.3. $d(L) = |\det B|$ is an invariant over different bases B for the lattice L.

Geometrically, we can think of $|\det B|$ as the area of a parallelogram in 2-dimensional space. In n-dimensional space, this corresponds to the volume of the parallelepiped with vertices from the set generated by $\sum_{i=1}^{n} \{0, 1\} \mathbf{b_i}$.

Theorem 1.4. *A set of linearly independent vectors $\{\mathbf{b_1}, \ldots, \mathbf{b_n}\} \subseteq L$ is a basis if and only if there is no element of the lattice in the interior of the corresponding parallelepiped.*

2 Review of Linear Algebra Concepts

Definition 2.1. If $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$, then their *inner product* is

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Definition 2.2. The *Euclidean length* of a vector $\mathbf{x}$ is

$$\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}.$$

2.1 Some useful properties of inner products

1. $\langle \mathbf{x}, \mathbf{x} \rangle = \|\mathbf{x}\|^2$.

2. $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ if and only if $\mathbf{x}$ and $\mathbf{y}$ are orthogonal.

3. $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

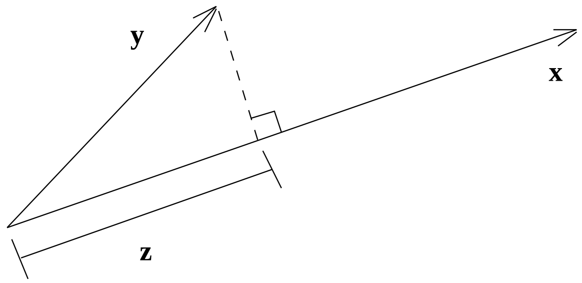

Figure 1: Orthogonal projection of $\mathbf{y}$ onto $\mathbf{x}$ in 2-dimensional space.

4. $\langle a\mathbf{x}, b\mathbf{y}\rangle = ab\langle \mathbf{x}, \mathbf{y}\rangle$, where $a, b \in \mathbb{R}$.

5. $\langle \mathbf{x}, \mathbf{y}+\mathbf{z}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle + \langle \mathbf{x}, \mathbf{z}\rangle$.

6. $\langle \mathbf{x}, \mathbf{y}\rangle = \|\mathbf{x}\| \cdot \|\mathbf{z}\|$, where $\mathbf{z}$ is the projection of $\mathbf{y}$ onto $\mathbf{x}$ (see Figure 1 for an example in 2-dimensional space). If they are orthogonal, then $\|\mathbf{z}\| = 0$.

3 Short Vectors and Orthogonal Bases

A given lattice L may have many different bases. Some of these bases are "better" than others, as shown in the following example.

Example 3.1. Let L be the integer lattice in $\mathbb{R}^2$. L has a standard basis with matrix representation

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Adding 100 times the first row of B_1 to the second row, we obtain another basis with matrix representation

$$B_2 = \begin{pmatrix} 1 & 0 \\ 100 & 1 \end{pmatrix}.$$

Adding 33 times the second row of B_2 to the first row, we obtain a third basis with matrix representation

$$B_3 = \begin{pmatrix} 3301 & 33 \\ 100 & 1 \end{pmatrix}.$$

In many applications, we want to find a *short* vector in L. Intuitively, a short vector is an element $\mathbf{v} \in L$ such that $\|\mathbf{v}\|$ is small. This notion will be made more precise later.

The basis B_1 is "nice", because it consists of short, orthogonal vectors. The basis B_3 is "lousy", because it consists of long vectors that are close to being in the same direction. In any basis for L, the area of the parallelogram formed by the two vectors in the basis must be 1. It follows that a basis in which the basis elements are nearly orthogonal will have "short" vectors, and a basis in which the basis elements are nearly parallel will have "long" vectors. This intuitive observation is true for lattices in higher dimensions as well.

4 Gram-Schmidt Orthogonalization

Given any basis $\{\mathbf{b_1}, \ldots, \mathbf{b_n}\}$ for a subspace of $\mathbb{R}^m$, the Gram-Schmidt algorithm produces an orthogonal basis $\{\mathbf{b_1^*}, \ldots, \mathbf{b_n^*}\}$ for the same subspace. The elements in an orthogonal basis satisfy $\langle \mathbf{b_i^*}, \mathbf{b_j^*} \rangle = 0$ for all $i \neq j$. We create the orthogonal basis by setting

$$\begin{array}{rcl}
\mathbf{b_1^*} & \leftarrow & \mathbf{b_1} \\
\mathbf{b_2^*} & \leftarrow & \mathbf{b_2} - \dfrac{\langle \mathbf{b_2}, \mathbf{b_1^*} \rangle}{\langle \mathbf{b_1^*}, \mathbf{b_1^*} \rangle} \mathbf{b_1^*} \\
\mathbf{b_3^*} & \leftarrow & \mathbf{b_3} - \dfrac{\langle \mathbf{b_3}, \mathbf{b_1^*} \rangle}{\langle \mathbf{b_1^*}, \mathbf{b_1^*} \rangle} \mathbf{b_1^*} - \dfrac{\langle \mathbf{b_2}, \mathbf{b_1^*} \rangle}{\langle \mathbf{b_1^*}, \mathbf{b_1^*} \rangle} \mathbf{b_1^*} \\
\vdots & \vdots & \vdots \\
\mathbf{b_i^*} & \leftarrow & \mathbf{b_i} - \displaystyle\sum_{j-1}^{i-1} \dfrac{\langle \mathbf{b_i}, \mathbf{b_j^*} \rangle}{\langle \mathbf{b_j^*}, \mathbf{b_j^*} \rangle} \mathbf{b_j^*}
\end{array}$$

We can also rewrite the relations above as

$$\mathbf{b_i} = \mathbf{b_i^*} + \sum_{j=1}^{i-1} \frac{\langle \mathbf{b_i}, \mathbf{b_j^*} \rangle}{\langle \mathbf{b_j^*}, \mathbf{b_j^*} \rangle} \mathbf{b_j^*}.$$

Define $\mu_{ii} = 1$, and define

$$\mu_{ij} = \frac{\langle \mathbf{b_i}, \mathbf{b_j^*} \rangle}{\langle \mathbf{b_j^*}, \mathbf{b_j^*} \rangle}$$

for $1 \leq j < i \leq n$. Intuitively, the quantities $|\mu_{ij}|$ measure how close the original basis is to being orthogonal. In particular, each μ_{ij} is 0 precisely when $\mathbf{b_i}$ and $\mathbf{b_j^*}$ are orthogonal.

5 Two-dimensional lattices

The algorithm in this section comes from Kannan's paper [1]. We start with a basis $\{\mathbf{b_1}, \mathbf{b_2}\}$ for a lattice L. We want to get a basis $\{\mathbf{b_1'}, \mathbf{b_2'}\}$ for L in which $\mathbf{b_1'}$ is "short". Note that, in this particular case, the Gram-Schmidt algorithm sets $\mathbf{b_1^*} = \mathbf{b_1}$ and $\mathbf{b_2^*} = \mathbf{b_2} - \mu_{21}\mathbf{b_1^*}$, where $\mu_{21} = \langle \mathbf{b_1}, \mathbf{b_2} \rangle / \langle \mathbf{b_1}, \mathbf{b_1} \rangle$. Unfortunately, while $\{\mathbf{b_1^*}, \mathbf{b_2^*}\}$ is a basis for the *subspace* spanned by $\{\mathbf{b_1}, \mathbf{b_2}\}$, it is not a basis for the lattice L unless μ_{21} happens to be an integer. So, let m be the integer closest to μ_{21}, and set

$$\begin{array}{rcl}
\mathbf{b_1'} & = & \mathbf{b_1} \\
\mathbf{b_2'} & = & \mathbf{b_2} - m\mathbf{b_1}.
\end{array}$$

Then

$$\begin{array}{rcl}
|\langle \mathbf{b_1'}, \mathbf{b_2'} \rangle| & = & |\langle \mathbf{b_2} - m\mathbf{b_1}, \mathbf{b_1} \rangle| \\
& = & |\langle \mathbf{b_2}, \mathbf{b_1} \rangle - \langle m\mathbf{b_1}, \mathbf{b_1} \rangle| \\
& = & |\mu_{21}\langle \mathbf{b_1}, \mathbf{b_1} \rangle - m\langle \mathbf{b_1}, \mathbf{b_1} \rangle| \\
& = & |\mu_{21} - m| \cdot \|\mathbf{b_1}\|^2 \leq \dfrac{1}{2}\|\mathbf{b_1}\|^2.
\end{array}$$

```
repeat
    swap $\mathbf{b_1}$ and $\mathbf{b_2}$. { Now $\|\mathbf{b_1}\| \le \|\mathbf{b_2}\|$. }
    $\mu_{21} \leftarrow \frac{\langle \mathbf{b_2}, \mathbf{b_1} \rangle}{\langle \mathbf{b_1}, \mathbf{b_1} \rangle}$.
    $m \leftarrow$ the unique integer in $\left(\mu_{21} - \frac{1}{2}, \mu_{21} + \frac{1}{2}\right]$.
    $\mathbf{b_2'} \leftarrow \mathbf{b_2} - m\mathbf{b_1}$.
        { Now $\mathbf{b_1}$ and $\mathbf{b_2'}$ form a basis for the lattice,
          and the angle between these vectors is at least $60^\circ$. }
    $\mathbf{b_2} \leftarrow \mathbf{b_2'}$.
until $\|\mathbf{b_1}\| \le \|\mathbf{b_2}\|$.
return $\{\mathbf{b_1}, \mathbf{b_2}\}$.
```

Figure 2: The 60° algorithm

In words, this inequality means that the length of the projection of $\mathbf{b_2'}$ in the direction of $\mathbf{b_1'}$ is at most half the length of $\mathbf{b_1'}$. Hence, the angle between $\mathbf{b_2'}$ and $\mathbf{b_1'}$ is in the range $[60^\circ, 120^\circ]$ or $[240^\circ, 300^\circ]$.

These ideas lead to the algorithm in Figure 2. Assume that the initial vectors satisfy $\|\mathbf{b_1}\| \ge \|\mathbf{b_2}\|$.

Note that this algorithm does terminate, since the values of $\|\mathbf{b_2}\|$ at the end of each loop iteration form a strictly decreasing sequence of positive integers, which cannot continue indefinitely.

Now, if α is the angle between $\mathbf{b_1}$ and $\mathbf{b_2}$, then

$$d(L) = \left| \det \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \end{pmatrix} \right| = \|\mathbf{b_1}\| \cdot \|\mathbf{b_2}\| \cdot |\sin\alpha|.$$

Since $60^\circ \le \alpha \le 120^\circ$ or $240^\circ \le \alpha \le 300^\circ$, we know that $|\sin\alpha| \ge \sqrt{3}/2$. So $d(L) \ge \|\mathbf{b_1}\| \cdot \|\mathbf{b_2}\| \cdot \sqrt{3}/2$, and $\|\mathbf{b_1}\| \cdot \|\mathbf{b_2}\| \le 2d(L)/\sqrt{3}$. Since $\|\mathbf{b_1}\| \le \|\mathbf{b_2}\|$ when the algorithm terminates, we conclude that

$$\|\mathbf{b_1}\| \le \left(\frac{d(L)}{\sqrt{3}/2} \right)^{1/2}.$$

We can use this inequality as the definition of what it means for $\mathbf{b_1}$ to be a *short vector* relative to the lattice L.

Example 5.1. Given $\mathbf{b}_1 = (9, -7)$ and $\mathbf{b}_2 = (7, -6)$:
Swap the vectors: $\mathbf{b}_1 = (7, -6)$, $\mathbf{b}_2 = (9, -7)$.
$\mu_{21} = \frac{63+42}{49+36} = \frac{105}{85}$.
The closest integer is 1; $m = 1$.
$\mathbf{b_2} = \mathbf{b}'_2 = (9, -7) - 1(7, -6) = (2, -1)$.
Is $\|\mathbf{b}_1\| \le \|\mathbf{b}_2\|$? No; repeat.
Swap the vectors: $\mathbf{b}_1 = (2, -1)$, $\mathbf{b}_2 = (7, -6)$.
$\mu_{21} = \frac{14+6}{4+1} = 4$.
$\mathbf{b_2} = \mathbf{b}'_2 = (7, -6) - 4(2, -1) = (-1, -2)$.
Is $\|\mathbf{b}_1\| \le \|\mathbf{b}_2\|$? Yes; return $\mathbf{b}_1$ and $\mathbf{b}_2$ as the basis.
Finally, verify that this agrees with the stated bound:
$\|\mathbf{b}_1\| = \sqrt{5} \le (\frac{d(L)}{\sqrt{3}/2})^{1/2} = (\frac{\cdot 5}{\sqrt{3}/2})^{1/2}$.

6 "Short" Vectors in the n-Dimensional Case

Theorem 6.1. *(Minkowski's Theorem — see Kannan's paper [2])*
If S is a closed, convex, symmetric (about the origin) set in $\mathbb{R}^n$ and has volume at least 2^n, then S contains at least one nonzero point of the integer lattice, $\mathbb{Z}^n - \{0\}$.

We define the following properties of S:

1. The boundary of a *convex* set forms a convex shape.

2. A *closed* set contains its perimeter and all interior points.

3. If a set A is *symmetric* about the origin, then for any $\mathbf{v} \in A$, $-\mathbf{v} \in A$.

Additionally, a set that contains the interval $[-1, 1]$, along each of n dimensions, has volume 2^n.

Theorem 6.2. *(Kannan's Theorem [1])*
If L is an n-dimensional lattice, then L contains a nonzero element $\mathbf{v}$ such that

$$\|\mathbf{v}\| \leq \sqrt{n}(d(L))^{1/n}.$$

This theorem provides us with a definition for "short" vectors in n dimensions. It employs Minkowski's theorem but does not provide an algorithm.

Proof. Let $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ be a basis of a lattice L and let

$$B = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_n \end{pmatrix}.$$

Define $T = \{(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) : -d(L)^{1/n} \leq \mathbf{x}_i \leq d(L)^{1/n}\}$. T has volume $2^n d(L)$. T is closed, convex, and symmetric. Hence, so is TB^{-1}. So, TB^{-1} has volume $2^n d(L)/d(L) = 2^n$. By Minkowski's Theorem, there is a $\mathbf{y} \in TB^{-1} \cap \mathbb{Z}^n - \{\mathbf{0}\}$. Then $\mathbf{v} = \mathbf{y}B$ is a nonzero element of $T \cap L - \{\mathbf{0}\}$. The longest vector in T is $(1, 1, \ldots, 1)d(L)^{1/n}$, and it has length $\sqrt{n}(d(L))^{1/n}$. Hence, since $\mathbf{v} \in T$, $\|\mathbf{v}\| \leq \sqrt{n}(d(L))^{1/n}$. □

References

[1] R. Kannan, *Lattices, basis reduction, and the shortest vector problem*, in Theory of Algorithms (Pécs, 1984), vol. 44 of Colloq. Math. Soc. Janos Bolyai, 1984, pp. 283–311.

[2] R. Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Research, 12 (No 3) (1987), pp. 415–439.

[3] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, eds., *Handbook of Applied Cryptography*, CRC Press, Boca, Raton, 1997.