Day 3: Higher Dimensions

Recall our guiding question:

Given a basis, what are the shortest vectors in the lattice generated by this basis?

Yesterday we found an algorithm to solve this question in 2 dimensions.

Definition

We will say that a 2-dimensional basis $\{\mathbf{u}, \mathbf{v}\}$ is **reduced** if $\|\mathbf{u}\| \leq \|\mathbf{v}\|$ and $\|\mathbf{v}\| \leq \|\mathbf{v} + n\mathbf{u}\|$ for all integers n.

Given a basis $\{\mathbf{u}, \mathbf{v}\}$, we can produce a reduced basis that generates the same lattice by alternating between the following two steps:

1. ("Swap") If $\|\mathbf{u}\| > \|\mathbf{v}\|$, then swap $\mathbf{u}$ and $\mathbf{v}$.
2. ("Slide") If $\|\mathbf{v}\| > \|\mathbf{v} + n\mathbf{u}\|$ for some integer n, replace $\mathbf{v}$ with the vector $\mathbf{v} + n\mathbf{u}$ such that $\|\mathbf{v} + n\mathbf{u}\|$ is as small as possible.

If neither step can be performed, then the basis is reduced. The algorithm must terminate because the vectors involved will get shorter at every sliding step, and there are only finitely many lattice vectors shorter than a given bound L.[1] And once $\{\mathbf{u}, \mathbf{v}\}$ is reduced, $\mathbf{u}$ is the shortest lattice vector!

Moving up in Dimension

What happens if we have a 3-D lattice? We might consider saying that a basis is reduced if every pair is reduced; this would imply that it is impossible to get a better basis by sliding any basis vector in the direction of any other basis vector. Unfortunately, a basis that is "reduced" in this sense can still be hiding a "surprise" short vector:

$$\mathbf{b}_1 = \begin{pmatrix} 1 \\ 0 \\ -10^{-6} \end{pmatrix}, \mathbf{b}_2 = \begin{pmatrix} 1/2 \\ \sqrt{3}/2 \\ 2 \cdot 10^{-6} \end{pmatrix}, \mathbf{b}_3 = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \\ -3 \cdot 10^{-6} \end{pmatrix}, \mathbf{b}_2 - \mathbf{b}_1 - \mathbf{b}_3 = \begin{pmatrix} 0 \\ 0 \\ 6 \cdot 10^{-6} \end{pmatrix}.$$

Could we have predicted the existence of this short vector just from looking at $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$? That's the question we will be exploring today.

[1] To prove this, suppose the angle between $\mathbf{u}$ and $\mathbf{v}$ is θ, and use the law of cosines to show that

$$\|a\mathbf{u} + b\mathbf{v}\|^2 \geq (1 - |\cos\theta|)(a^2\|\mathbf{u}\|^2 + b^2\|\mathbf{v}\|^2) \geq (a^2 + b^2)c,$$

where c is some positive constant depending only on $\mathbf{u}$ and $\mathbf{v}$. So $\|a\mathbf{u}+b\mathbf{v}\| < L$ can only occur if $a^2+b^2 < L/c$.

Definitions

A set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^n$ is a **basis** if any vector in $\mathbb{R}^n$ can be written $r_1\mathbf{b}_1 + \cdots + r_n\mathbf{b}_n$ for exactly one choice of real numbers $r_1, \ldots, r_n$.

Given a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, the **lattice generated by this basis** is the set

$$\mathcal{L} = \{a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

The fundamental parallelotope of the basis is the set

$$P = \{r_1\mathbf{b}_1 + r_2\mathbf{b}_2 + \cdots + r_n\mathbf{b}_n \mid r_1, r_2, \ldots, r_n \in [0, 1)\}.$$

Minkowski's Theorem

Let's work towards a proof of the following result. A subset S of $\mathbb{R}^n$ is *symmetric* if whenever $\mathbf{v} \in S$, then also $-\mathbf{v} \in S$. The set S is *convex* if whenever $\mathbf{v}, \mathbf{w} \in S$, all vectors on the line segment connecting $\mathbf{v}$ to $\mathbf{w}$ are also in S.

Theorem 1 (Minkowski 1889)

Let S be a convex, symmetric subset of $\mathbb{R}^n$, and let P be the fundamental parallelotope of a basis generating some lattice $\mathcal{L}$. If $\text{Vol}(S) > 2^n\text{Vol}(P)$, then S contains a nonzero element of $\mathcal{L}$.

Exploration 2

We can define a function $\mathbb{R}^n \to P$ as follows: if a vector can be written as $\mathbf{l} + \mathbf{p}$ for $\mathbf{l} \in \mathcal{L}$ and $\mathbf{p} \in P$, send $\mathbf{l} + \mathbf{p}$ to $\mathbf{p}$. Describe this function geometrically.

Exploration 3

Let $S/2$ denote the set S shrunk down by a factor of 2. If $\text{Vol}(S/2) > \text{Vol}(P)$, conclude that there must be two vectors in $S/2$ which differ by a nonzero lattice vector $\mathbf{l}$.

Exploration 4

Use properties of S to show that $\frac{1}{2}\mathbf{l} \in S/2$. Then scale back up and finish the proof.

How does Minkowski's Theorem help us with the short vector question? The key insight is that we can turn a *length* question (is there a vector with length at most d) into a *volume* question (is there a vector in the ball of radius d).

Exploration 5

Prove that the n-dimensional ball of radius $\sqrt{n}$ has volume greater than 2^n. Use this to prove Corollary 6.

Corollary 6 (of Theorem 1)

Let P be a fundamental parallelotope for $\mathcal{L}$. Then there exists a nonzero vector $\mathbf{l} \in \mathcal{L}$ with

$$\|\mathbf{l}\| \leq \sqrt{n}\mathrm{Vol}(P)^{1/n}.$$

Exploration 7

Consider the basis discussed at the beginning of this sheet. The parallelotope it generates has volume $3\sqrt{3}/10^6$.[a] Does Corollary 6 predict the existence of the short vector we found? How far off is the bound?

[a] If you want to know how to compute this, see Fact 12 in the Optional Exploration section.

Successive Minima and Minkowski's Second Theorem

Minkowski's Theorem is an upper bound: it guarantees the existence of a short vector in our lattice. A lower bound would be nice too (to tell us that the shortest vector can't be *toooo* short), but unfortunately the volume of the fundamental parallelotope is not enough to give us such a result:

Exploration 8

Find a basis in $\mathbb{R}^2$ such that the area of the fundamental parallelogram is 1, but the length of the shortest vector is very very very very small.

The issue is that you can make one vector extremely small without changing the volume of the fundamental parallelotope, as long as you compensate by making other vectors longer.

Definition

The **succesive minima** of a lattice, $\lambda_1 \leq \cdots \leq \lambda_n$, are defined by the following property: λ_i is the smallest number such that there exist at least i *linearly independent* vectors of length at most λ_i.

If you picture a ball with growing radius, then λ_i represents the moment that the ball swallows up a vector pointing in an i^{th} new direction. In particular, λ_1 is the length of the shortest nonzero vector in the lattice. So Minkowski's (first) theorem tells us that if B is an n-dimensional ball of radius 1, then

$$\lambda_1^n \text{Vol}(B) \leq 2^n \text{Vol}(P).$$

Minkowski's Second Theorem is similar, except that it uses all the successive minima.

Theorem 9 (Minkowski 1896)

Let B be an n-dimensional ball of radius 1, P be the fundamental parallelotope of a lattice $\mathcal{L}$, and $\lambda_1, \ldots, \lambda_n$ the successive minima of $\mathcal{L}$. Then

$$\frac{1}{n!} 2^n \text{Vol}(P) \leq \lambda_1 \cdots \lambda_n \text{Vol}(B) \leq 2^n \text{Vol}(P).$$

This gives us quite a bit of additional information about the "shape" of our lattice.

Exploration 10

Looking again at the basis $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ from the beginning of this sheet, we found a very short vector $\mathbf{x}$. Prove that there are no other "surprise" short vectors in the lattice. Specifically, any vector that is not a multiple of $\mathbf{x}$ must have length at least 0.275. (Hint: The vectors we already know about give upper bounds for λ_1 and λ_3.)

Optional Exploration: Proving the Lower Bound

The upper bound in Theorem 9 is rather deep and involved, but we can prove the lower bound! Let $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be vectors in a lattice $\mathcal{L}$ such that $\mathbf{x}_i$ has length λ_i.

Exploration 11

We took $\mathbf{x}_1, \ldots, \mathbf{x}_n$ to be a set of linearly independent vectors that are as short as possible, so you might expect them to form a basis for $\mathcal{L}$. This is true in 2 dimensions: if $\mathcal{L}$ is generated by a reduced basis $\{\mathbf{u}, \mathbf{v}\}$, then $\lambda_1 = \|\mathbf{u}\|$ and $\lambda_2 = \|\mathbf{v}\|$.
But consider the lattice $\mathcal{L}$ in $\mathbb{R}^5$ generated by

$$\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1/2\\1/2\\1/2\\1/2\\1/2\end{pmatrix}.$$

Show that $\lambda_1 = \cdots = \lambda_5 = 1$, but any basis for $\mathcal{L}$ must contain a vector of length at least $\sqrt{5}/2 > 1$. You can't get a basis just by taking the shortest linearly independent vectors! Low-dimensional intuition fails us here; high-dimensional lattices are *weird*.

For the next exploration we'll need the following fact (this is just explaining what the determinant of a matrix means geometrically).

Fact 12

The parallelotope generated by $\mathbf{v}_1, \ldots, \mathbf{v}_n$,

$$\{r_1\mathbf{v}_1 + r_2\mathbf{v}_2 + \cdots + r_n\mathbf{v}_n \mid r_1, r_2, \ldots, r_n \in [0,1]\},$$

has volume equal to $|\det V|$, where

$$V = \begin{pmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \\ | & | & & | \end{pmatrix} = \begin{pmatrix} v_{11} & v_{21} & \cdots & v_{n1} \\ v_{12} & v_{21} & \cdots & v_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & \cdots & v_{nn} \end{pmatrix}$$

has each vector $\mathbf{v}_i$ as a column.

See `https://textbooks.math.gatech.edu/ila/determinants-volumes.html` for a proof.

Exploration 13

If $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a basis for $\mathcal{L}$, show that we can write

$$\begin{pmatrix} | & | & & | \\ \mathbf{x}_1 & \mathbf{x}_2 & \cdots & \mathbf{x}_n \\ | & | & & | \end{pmatrix} = \begin{pmatrix} | & | & & | \\ \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_n \\ | & | & & | \end{pmatrix} C$$

for some matrix C with integer entries. Letting P' denote the parallelotope generated by $\mathbf{x}_1, \ldots, \mathbf{x}_n$, show that $\mathrm{Vol}(P') \geq \mathrm{Vol}(P)$.

Exploration 14

Consider the region T in $\mathbb{R}^n$ bounded by vertices at $\pm\mathbf{x}_i$ for all i. Compute the volume of T in terms of the volume of P'. (First do this for the standard basis $\mathbf{x}_1 = (1, 0, 0, \ldots), \mathbf{x}_2 = (0, 1, 0, \ldots), \ldots$, starting with 2 and 3 dimensions to figure out what's going on. Then apply a linear map to get it to work for more general $\mathbf{x}_1, \ldots, \mathbf{x}_n$.)

Exploration 15

Consider the region T' in $\mathbb{R}^n$ bounded by vertices at $\pm\mathbf{x}_i/\lambda_i$ for all i. Show that T' is contained in B. How is the volume of T' related to the volume of T?