Day 2: Lattice Basis Reduction

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

The main reason $\{\mathbf{u}, \mathbf{v}\} = \{(1,0), (0,1)\}$ is so nice to work with is because it's an *orthogonal* (90°) basis. This means that we can just compute the lengths of lattice points using the Pythagorean Theorem: when $\mathbf{u}$ and $\mathbf{v}$ are orthogonal, we have

$$\|a\mathbf{u} + b\mathbf{v}\|^2 = a^2\|\mathbf{u}\|^2 + b^2\|\mathbf{v}\|^2,$$

where $\|\cdot\|$ denotes taking the length of the vector. This implies that, unlike for some bases, there are no "surprise" short vectors; the only short vectors are those with small coefficients for $\mathbf{u}$ and $\mathbf{v}$.

Unfortunately, most lattices will not have orthogonal bases. But we can try to get as close as possible!

Attempting Orthogonalization

Exploration 1

For any integer n, prove that $\{\mathbf{u}, \mathbf{v}\}$ and $\{\mathbf{u}, \mathbf{v} + n\mathbf{u}\}$ generate the same lattice.

This gives us a valuable tool for finding new bases: we can slide one basis vector along the direction of another basis vector. Doing this allows us to make the angle between the basis vectors closer to a right angle.

Exploration 2

Show that the same integer n solves both of the following problems:

- Find n such that $\mathbf{v} + n\mathbf{u}$ is as short as possible.
- Find n such that the angle between $\mathbf{u}$ and $\mathbf{v} + n\mathbf{u}$ is as close to 90° as possible.

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.

Exploration 3

Suppose $\mathbf{u} = (1, 0)$. Draw the region in $\mathbb{R}^2$ containing all vectors $\mathbf{v}$ such that $\{\mathbf{u}, \mathbf{v}\}$ is a reduced basis. What will the region look like if you choose a different vector $\mathbf{u}$?

Reduced bases are almost as nice as orthogonal bases to work with. In particular, lengths are relatively predictable, and it is straightforward to find the shortest vectors:

Exploration 4

If $\{\mathbf{u}, \mathbf{v}\}$ is a reduced basis, prove that the squared length of any lattice vector $a\mathbf{u}+b\mathbf{v}$ is at least $\frac{1}{2}(a^2\|\mathbf{u}\|^2 + b^2\|\mathbf{v}\|^2)$. Use this to conclude that there is no nonzero lattice vector shorter than $\mathbf{u}$.

Exploration 5

Suppose $\mathbf{u} = (1, 0)$ and $\mathbf{v} = (\frac{9}{4}, \frac{1}{4})$. First make a prediction regarding the "shape" of the lattice this generates (i.e. is it square, triangular, rectangular?).

Now find an n that solves the problem from Exploration 2 for this lattice. Is $\{\mathbf{u}, \mathbf{v}+n\mathbf{u}\}$ reduced? If not, what more do you need to do to make it reduced?

Exploration 6

Describe an algorithm that takes a basis as input, and returns a reduced basis generating the same lattice. Why must your algorithm terminate?

(For the following explorations, you may want to have a method to do calculations with vectors; it's not necessary, but it might help speed things up. Click here for one option.)

Exploration 7

The mayor of Skewvillle (see Figure 1) is embarking on a massive construction project which will involve laying an entirely new road system. She wants to preserve the locations of all the intersections, but wants to minimize travel time between nearby intersections. What directions should the new roads be built in?

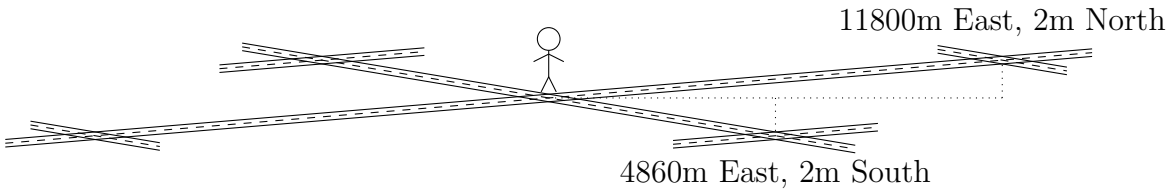

Figure 1: You and adjacent intersections (not to scale).

Unfortunately, if we try and extend this definition of "reduced" in a natural way to higher dimensions, things aren't as nice.

Exploration 8

Consider the basis

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

(written as column vectors). Show that each pair of basis vectors is reduced, but that the lattice generated by $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ contains a vector that is much shorter than any of the basis vectors.

Exploration 9 (Optional)

We've shown that every 2-D lattice has at least one reduced basis. In fact there will always be more than one (for example, if $\{\mathbf{u}, \mathbf{v}\}$ is a reduced basis then so is $\{\pm\mathbf{u}, \pm\mathbf{v}\}$). Add some extra constraints to the definition of "reduced" in order to guarantee that every lattice has *exactly one* reduced basis
(Hint: use the drawing from Exploration 5. Which choices of $\mathbf{v}$ will generate the same lattice? How will you pin down a specific choice for the vector $\mathbf{u}$? Be especially careful of the situation in which there are more than two vectors with the same shortest length)

Optional Exploration: Short Vectors in Number Theory

The problem of finding short vectors in a lattice has many applications. We'll explore a few of them here:

Exploration 10

Consider the lattice generated by the basis

$$\mathbf{u} = \begin{pmatrix} 1071 \\ 0 \end{pmatrix}, \mathbf{v} = \begin{pmatrix} 462 \\ 0.0001 \end{pmatrix}.$$

Explain why the reduced basis has the form

$$\begin{pmatrix} 0 \\ [\text{small}] \end{pmatrix}, \begin{pmatrix} \gcd(1071, 462) \\ [\text{small}] \end{pmatrix}.$$

Exploration 11

Consider the lattice generated by

$$\mathbf{u} = \begin{pmatrix} \pi \\ 0 \end{pmatrix}, \mathbf{v} = \begin{pmatrix} 1 \\ 0.0001 \end{pmatrix}.$$

If you can find a short lattice vector $a\mathbf{u} + b\mathbf{v}$, explain how this gives you a rational approximation to π. What could you change about the basis in order to find better approximations?

Exploration 12

Suppose we have a real number α that we believe is the root of some quadratic polynomial, but all we know is a decimal approximation: $\alpha \approx 0.4708709$. Explain how finding a short vector in the lattice generated by

$$\mathbf{u} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{v} = \begin{pmatrix} 0.4708709 \\ 0.0000001 \\ 0 \end{pmatrix}, \mathbf{w} = \begin{pmatrix} 0.4708709^2 \\ 0 \\ 0.0000001 \end{pmatrix}.$$

can be used to find a candidate for the mystery polynomial.