Day 1: 2-D Lattices and Bases

We're going to start by just playing around with lattices to get a feel for how they work. Go to the "lattice player" `https://stanford.edu/~jonlove/mc20/lattice-play.html`.

Definitions

You will see two pink vectors labeled **u** and **v**.[a] As long as they don't lie on the same line, they form a **lattice basis**.

The gray points are obtained by taking $m\mathbf{u} + n\mathbf{v}$ for various integers m and n. These are called **lattice points** or **lattice vectors**. The set of all of these points is "**the lattice generated by the basis** $\{\mathbf{u}, \mathbf{v}\}$."

The pink parallelogram is called the **fundamental parallelogram of the basis** $\{\mathbf{u}, \mathbf{v}\}$. It conatins every point in the interior, as well as every point on the edge connecting O to $\mathbf{u}$, and every point on the edge connecting O to $\mathbf{v}$. It does *not* contain the points on the other two edges.

[a] Bold letters for vectors, italic letters for numbers.

Explore the following questions in breakout rooms. (You can take turns sharing your screen, or one of you can share your screen and the others can use annotations to discuss.)

Exploration 1

Move **u** and **v** around. Make observations about how the fundamental parallelogram changes, and how the lattice changes. Can you find **u** and **v** very long, but generating a nonzero lattice vector which is very short? Can you find a basis with a really funky stretched out fundamental parallelogram, but which generates a nice, even lattice?

Exploration 2

"The entire plane is a jigsaw puzzle, where each puzzle piece is an identical copy of the fundamental parallelogram."
First try to understand this visually, then prove Proposition 3. Make sure everyone in your group is satisfied; even if you figure it out, explaining your ideas clearly is a skill worth practicing! (Hint: the hard part is making the definitions precise.)

Proposition 3

Suppose $\mathbf{u}$ and $\mathbf{v}$ are linearly independent vectors in $\mathbb{R}^2$. Prove that every point in the plane can be written uniquely in the form $\mathbf{l} + \mathbf{p}$, where $\mathbf{l}$ is in the lattice generated by $\mathbf{u}$ and $\mathbf{v}$, and $\mathbf{p}$ is in the fundamental parallelogram of $\mathbf{u}$ and $\mathbf{v}$.

Definition

The **standard lattice** or **integer lattice** is the set of points

$$\mathbb{Z}^2 := \{(m, n) \mid m, n \in \mathbb{Z}\}.$$

For example, if $\mathbf{p} = (1, 0)$ and $\mathbf{q} = (0, 1)$, then $\{\mathbf{p}, \mathbf{q}\}$ generates $\mathbb{Z}^2$.

Exploration 4

Find as many different choices of $\mathbf{u}$ and $\mathbf{v}$ as possible that generate $\mathbb{Z}^2$. (For example, what happens if you set $\mathbf{u} = (5, 2)$ and $\mathbf{v} = (2, 1)$?) Come up with a hypothesis for a criterion that determines whether a basis generates $\mathbb{Z}^2$.

Exploration 5

Now let's start to use the green and blue sliders! Choose a basis $\mathbf{u}$ and $\mathbf{v}$ that generates $\mathbb{Z}^2$ (from Exploration 4), and look for integers a, b, c, and d such that $a\mathbf{u} + b\mathbf{v} = (1, 0)$ and $c\mathbf{u} + d\mathbf{v} = (0, 1)$. Repeat with different choices of $\{\mathbf{u}, \mathbf{v}\}$, and try to predict what a, b, c, d will work in each case.

Exploration 6

What algebraic relationships must be satisfied by the variables a, b, c, d and the components of $\mathbf{u}$ and $\mathbf{v}$ in order to guarantee that $a\mathbf{u} + b\mathbf{v} = (1, 0)$ and $c\mathbf{u} + d\mathbf{v} = (0, 1)$? Can you express these relationships in a single equation?

Exploration 7

Generalize your results to other lattices. That is, suppose a lattice is generated by a basis $\{\mathbf{u}, \mathbf{v}\}$, and the same lattice is also generated by $\{\mathbf{p}, \mathbf{q}\}$ (the previous explorations were considering the special case $\mathbf{p} = (1, 0)$ and $\mathbf{q} = (0, 1)$). What relationship must be satisfied by $\mathbf{u}, \mathbf{v}, \mathbf{p}, \mathbf{q}$?
(Hint: each basis appears in the lattice generated by the other)

Guiding question going forward:

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

For some bases (like $\{(1, 0), (0, 1)\}$) this is easy, but it's not always so straightforward.

Exploration 8

What makes the basis $\{(1, 0), (0, 1)\}$ so easy to work with? Are there other bases for which it's easy to identify the short lattice vectors?

Optional Exploration: Lattice Points and Polygons

Exploration 9

Prove Theorem 10 and its corollary below. For the theorem, start with easy cases and build your way up to more complicated ones.

Theorem 10 (Pick's Theorem)

If the vertices of a polygon lie on a lattice $\mathcal{L}$ in $\mathbb{R}^2$, then the area of the polygon is

$$\left(i + \frac{b}{2} - 1\right) f,$$

where

- i is the number of points in $\mathcal{L}$ in the interior of the polygon,
- b is the number of points in $\mathcal{L}$ on the boundary of the polygon, and
- f is the area of the fundamental parallelogram of $\mathcal{L}$.

Corollary 11

Let S be any bounded convex subset of $\mathbb{R}^2$, and $\mathcal{L}$ be any lattice. Then the number of lattice points in S is at most

$$\frac{\text{Area}(S)}{f} + \frac{\text{Perimeter}(S)}{2\ell} + 1,$$

where f is the area of the fundamental parallelogram of $\mathcal{L}$, and ℓ is the length of the shortest nonzero vector in $\mathcal{L}$.
(You may use the following fact without proof: if A and B are convex subsets of $\mathbb{R}^2$ and A is contained in B, then the perimeter of A is at most the perimeter of B.)

Exploration 12

Explain why each of the three individual terms in Corollary 11 are necessary. That is, if you remove any individual term from the sum, describe a set S that would contain more lattice points than the modified sum would predict.

Exploration 13

Does a version of Pick's Theorem hold in 3 dimensions?

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* 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

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

Exploration 6

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?

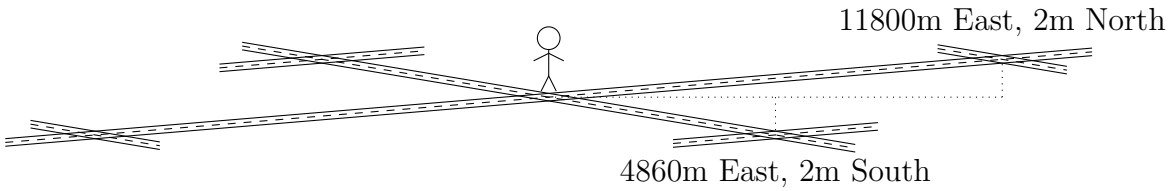


Figure 1: You and adjacent intersections (not to scale).

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

Exploration 7

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 8 (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 3. 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 9

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 10

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 11

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.

Day 3: Higher Dimensions

Recall our guiding question:

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

We have an algorithm to solve this question in 2 dimensions, using the notion of a "reduced basis." But as soon as we increase the dimension, we can have bases that are reduced (no basis vector can be shortened by sliding it along the direction of another basis vector) but are still hiding short vectors in the lattice they generate, for example:

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

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 parallelepiped 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's Theorem)

Let S be a convex, symmetrix subset of $\mathbb{R}^n$, and let P be the fundamental parallelepiped 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 parallelepiped for $\mathcal{L}$. Then there exists a nonzero vector $\mathbf{l} \in \mathcal{L}$ with

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

Exploration 7

Consider the basis discussed at the beginning of this sheet. The parallelepiped 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 parallelepiped 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 parallelepiped, 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's Second Theorem)

Let B be an n-dimensional ball of radius 1, P be the fundamental parallelepiped 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.

Optional Exploration: 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*.

Fact 12

The parallelepiped 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 parallelepiped 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'. (As a warm-up, compare the volume of the region bounded by the vertices $\mathbf{0}, \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ to the volume of the parallelepiped generated by $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$. Starting with 2 or 3 dimensions might help.)

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?

Day 4: LLL Reduction

> "Computational aspects of geometry of numbers have been revolutionized by the Lenstra-Lenstra-Lovász lattice reduction algorithm (LLL), which has led to breakthroughs in fields as diverse as computer algebra, cryptology, and algorithmic number theory. After its publication in 1982, LLL was immediately recognized as one of the most important algorithmic achievements of the twentieth century, because of its broad applicability and apparent simplicity."
>
> ∼ Phong Q. Nguyen and Brigitte Vallée (2009)

We need a better notion of "reduced" bases for dimensions above 2. For instance, let's use our example from before:

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

How could we have predicted the existence of a short vector? One way (discussed yesterday) is Minkowski's Theorem, but this couldn't have prepared us for just how short the shortest vector is. Another approach is to notice that $\mathbf{b}_3$ is *extremely close* to the plane spanned by $\mathbf{b}_1$ and $\mathbf{b}_2$. In other words, the only contribution from $\mathbf{b}_3$ in a *new* direction is very very small — and we might be able to isolate this short piece by subtracting an appropriate combination of $\mathbf{b}_1$ and $\mathbf{b}_2$.

To quantify this idea (that a vector is close to the space spanned by the previous vectors), we can use *projections*.

Definitions

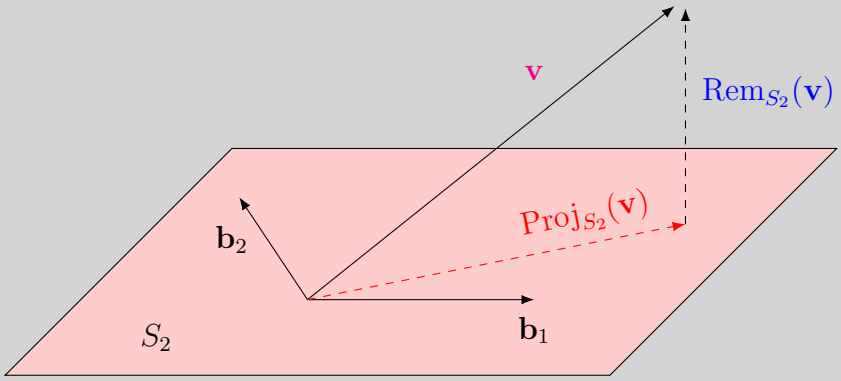
Suppose $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a basis for $\mathbb{R}^n$. For each i from 1 to n, let S_i denote the **subspace spanned by the first i vectors**:

$$S_i = \{r_1\mathbf{b}_1 + \ldots + r_i\mathbf{b}_i \mid r_1, \ldots, r_i \in \mathbb{R}\}.$$

Given any vector $\mathbf{v} \in \mathbb{R}^n$, and any i, it can be decomposed uniquely as

$$\mathbf{v} = \text{Proj}_{S_i}(\mathbf{v}) + \text{Rem}_{S_i}(\mathbf{v}),$$

where $\text{Proj}_{S_i}(\mathbf{v})$ (the **projection** of $\mathbf{v}$ onto S_i) is contained in S_i, and $\text{Rem}_{S_i}(\mathbf{v})$ (the **remainder** of the projection of $\mathbf{v}$ onto S_i) is orthogonal to every vector in S_i.



(We also set $S_0 = \{\mathbf{0}\}$, so $\text{Proj}_{S_0}(\mathbf{v}) = \mathbf{0}$ and $\text{Rem}_{S_0}(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v}$.)

The remainder function $\text{Rem}_{S_i}(\mathbf{v})$ tells us what is *new* about the vector $\mathbf{v}$; it describes what $\mathbf{v}$ is contributing to the world that hasn't already been done by vectors in S_i. Let

$$\mathbf{b}_k^* = \text{Rem}_{S_{k-1}}(\mathbf{b}_k)$$

denote the "new contribution" from $\mathbf{b}_k$ (the remainder after projecting onto all the previous basis vectors). The vectors $\mathbf{b}_k^*$ will usually *not* be lattice vectors (except for $\mathbf{b}_1^*$), but they can be used to find a lower bound on the shortest vectors in a lattice!

Proposition 1

Let a lattice $\mathcal{L}$ be generated by $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Then every nonzero vector in $\mathcal{L}$ is longer than the minimum value of $\|\mathbf{b}_k^*\|$ over $k \in \{1, \ldots, n\}$.

Exploration 2

Given a lattice vector $a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n$, let a_j be the last nonzero coefficient. What is the remainder after projection onto S_{j-1}? Use this to prove Proposition 1.

Go to [link]

Exploration 3

Using the basis $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ from the start of this sheet, compute $\mathbf{b}_1^*$, $\mathbf{b}_2^*$, and $\mathbf{b}_3^*$. According to Proposition 1, what is the shortest possible length of a nonzero lattice vector?

Remember this definition?

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.

For higher dimensions, instead of comparing pairs of basis vectors, we will will compare the *new contributions* of basis vectors; that is, we will be comparing the *remainders* of basis vectors after removing the projections onto all previous vectors.

Definition

An n-dimensional basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ is **LLL-reduced** (with parameter $\delta = 1$) if the following are true for all $k = 2, \ldots, n$:

- $\|\text{Rem}_{S_{k-2}}(\mathbf{b}_{k-1})\| \leq \|\text{Rem}_{S_{k-2}}(\mathbf{b}_k)\|$,[a] and
- $\|\text{Rem}_{S_{i-1}}(\mathbf{b}_k)\| \leq \|\text{Rem}_{S_{i-1}}(\mathbf{b}_k) + n\text{Rem}_{S_{i-1}}(\mathbf{b}_i)\|$ for all $1 \leq i < k$ and all integers n.

[a] Careful: the first term is $\mathbf{b}_{k-1}^*$, but the second term is not $\mathbf{b}_k^*$. We're only projecting away the first $k-2$ vectors, not the first $k-1$.

Exploration 4

Is the basis $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ from the beginning of this sheet LLL-reduced? Why or why not?

Exploration 5

If a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is LLL-reduced, prove that $\|\mathbf{b}_k^*\| \geq \frac{\sqrt{3}}{2}\|\mathbf{b}_{k-1}^*\|$.

Exploration 6

Suppose $\mathbf{v}$ is any vector in $\mathbb{R}^n$, and $\mathbf{w}$ is a vector contained in S_i. How are $\text{Rem}_{S_i}(\mathbf{v})$ and $\text{Rem}_{S_i}(\mathbf{v}+\mathbf{w})$ related?
Now suppose that $\|\text{Rem}_{S_{i-1}}(\mathbf{b}_k)\|$ is smaller than $\|\text{Rem}_{S_{i-1}}(\mathbf{b}_k) + n\text{Rem}_{S_{i-1}}(\mathbf{b}_i)\|$ for all n. If you replace $\mathbf{b}_k$ with $\mathbf{b}_k + m\mathbf{b}_j$ for some $j < i$ and some integer m, show that this condition is still satisfied.

Day 5: Lattice-based Cryptography