CS 812
Lecture 35
Friday 4/17/20

Topic du jour: Introduction to Lattices

Reference: Hardy and Wright XIV, XXIV.

Background

What should number theory in higher dimensions look like? A good case can be made that the proper analog to the integers $\mathbf{Z}$ is the concept of lattice: roughly, a regular array of points that expands to fill space in all directions.

Once we have the idea of a lattice (exact definition forthcoming) we can ask how they are described, and among the many possible descriptions, which ones are best. This leads directly to the concept of lattice reduction. The root of this concept go back to the 18th century (at least), but it has many modern applications.

Key paper: Lenstra, Lenstra, Lovasz, Math. Annalen, v. 261, 1982, pp. 515-534. Among other things, this proves that polynomials in one variable over the rational numbers can be factored in polynomial time.

Lattices

Defn. A lattice L is a discrete additive subgroup of $\mathbf{R}^n$.

"Discrete" means that the points of L are separated. That is, there is some $\epsilon > 0$ such that if $x \in L$, the ball of radius ϵ around x contains no other point of L besides x itself.

To be an additive subgroup means that it is closed under addition, and multiplication by ± 1. (Therefore, it contains 0.)

Example: $\mathbf{Z}^2 = \{(a, b) : a, b \in \mathbf{Z}\}$ is a lattice contained in $\mathbf{R}^2$.

The discreteness condition is important. Within $\mathbf{R}$, the set of all integer linear combinations of 1 and $\sqrt{2}$ is isomorphic (as a group) to $\mathbf{Z}^2$, but it has points that are arbitrarily close together. (Can you prove this?)

Theorem: If $v_1, v_2, \ldots, v_n$ are vectors in $\mathbf{R}^n$ that are linearly independent over R, then the set of all integer linear combinations,

$$L = \{\sum_i x_i v_i : x_i \in \mathbf{Z}\}$$

is a lattice.

Proof: clearly this is a subgroup. To show it is discrete, we observe that $f(x_1, \ldots, x_n) = \sum_i x_i v_i$ is a continuous bijection from $\mathbf{R}^n$ to itself, mapping $\mathbf{Z}^n$ onto L. So L is discrete iff $\mathbf{Z}^n$ is. To show $\mathbf{Z}^n$ is discrete, let x be a vector of

integers and y any other such vector. By the usual distance formula, $|x - y| \geq 1$. So we can take $\epsilon = 1/2$.

Defn. A basis for L is a linearly independent subset $\{b_1, \ldots, b_n\}$ that generates L as an abelian group. That is,

$$L = \{\sum_i x_i b_i : x_i \in \mathbf{Z}\}$$

and $\sum x_i b_i = 0$ only when all $x_i = 0$.

Every lattice has many bases.

Example: One basis for $\mathbf{Z}^2$ is $\{(1,0),(0,1)\}$. Another is $\{(1,0),(a,1)\}$, for any integer a. It can be shown (exercise for you) that $\{(a,b),(c,d)\}$ is a basis for $\mathbf{Z}^2$ iff the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is invertible over $\mathbf{Z}$. That is, its determinant is ± 1.

Next question: Among all bases, can we identify one that is, in some sense, distinguished? Although this may be theoretically possible, there is no known fast algorithm to do it except for small dimensions.

The contribution of Lenstra, Lenstra, and Lovasz was to realize that for many purposes, it would be enough to get a "good" basis, not necessarily a canonical form. Before introducing their algorithm, we show what is possible for some small values of n.

Dimension 1

This is completely covered by theory we already know. Suppose $b_1, \ldots, b_r$ are integers. The lattice they generate is an ideal of $\mathbf{Z}$ (since closure under multiplication by integers is implied by closure under addition and subtraction), and we know all such ideals are principal. (This is a standard result, see any modern algebra book.) Therefore, if not all b_i are zero, a generator for the lattice of integer linear combinations of $b_1, \ldots, b_n$ is

$$d = \gcd(b_1, ..., b_n).$$

It is worth noticing that all lattices in $\mathbf{R}$ have the same "shape," since they consist of all integer multiples of some nonzero d. This only happens in dimension 1.

Dimension 2

This is a classic topic. We will think of L as a subset of $\mathbf{C}$, the complex numbers. To avoid degenerate cases, we assume that L has rank 2, that is, it contains two elements that are linearly independent over the reals. We also distinguish between the different orderings of a basis, so that $[b_1, b_2] \neq [b_2, b_1]$.

Defn: A basis $[b_1, b_2]$ of a lattice is called reduced if $b_1/b_2 \in D$, where

$$D = \{z \in \mathbf{C} : |z| \geq 1, \mathrm{Im}(z) > 0, -1/2 \leq \mathrm{Re}(z) < 1/2\}.$$

Before going on, you should take out some graph paper and draw a picture of D. It looks like vertical strip with a circular piece stamped out of the bottom.

Some people put further constraints on the points with $|z| = 1$. We'll ignore this fine point for now.

Theorem: Every rank-2 lattice in $\mathbf{C}$ has a reduced basis.

Proof: We first show that L contains a nonzero vector of minimum length. Choose a nonzero $v \in L$, and let $R = |v|$. The set

$$S = \{x \in L : |x| \leq R\}$$

is finite. (If not, a sequence chosen from L has a limit point, contradicting our assumption that $|x - y|$ is bounded below when x, y are distinct elements of L.) Choose b_1 to be a vector of minimum length from S. Next, we observe that b_1 can be extended to a basis. Take any basis $[c_1, c_2]$ for L. Then there are integers x, y for which $b_1 = xc_1 + yc_2$. These must be relatively prime (if not, b_1 wasn't minimal), so there are integers z, w such that

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

is invertible. (Use the extended Euclidean algorithm.) Let $b_2 = zc_1 + wc_2$. Because the matrix above is invertible, $[b_1, b_2]$ is also a basis.

Change b_2 to $-b_2$ if necessary, to make $\mathrm{Im}(b_2/b_1) > 0$. (This cannot equal 0, because then b_2 would be collinear with b_1.)

Now let $\hat{b}_2$ be the projection of b_2 onto the line generated by b_1. By subtracting an appropriate integer multiple of b_1 from b_2, we can make $\hat{b}_2$ lie within the segment $[b_1/2, b_1)$.

Explicitly, we have

$$\hat{b}_2 = \frac{(b_1, b_2)}{|b_1|^2} b_1,$$

where (b_1, b_2) is the usual inner product. Let

$$\mu = \left[\frac{(b_1, b_2)}{|b_1|^2} \right] - 1/2$$

where $[\,]$ is the greatest integer (floor) function. Then if we replace b_2 by $b_2 - \mu b_1$, the basis $[b_1, b_2]$ is reduced.

You will notice that the only nonconstructive part of this proof is the choice of a shortest vector in L. In the next lecture, we will give an algorithm to compute a

reduced basis for any 2-dimensional lattice, and prove that it runs in polynomial time.

A good example to consider is the Gaussian integers. These are the complex numbers $x + yi$, with x and y both (ordinary) integers. A reduced basis for this lattice is $[1, i]$. (What are the other ones?) The Gaussian integers inherit a (commutative) ring structure from $\mathbf{C}$, and this ring is a Euclidean domain. See Hardy and Wright for discussion of this.

Reduced Bases and Shortest Vectors

Theorem: If $[b_1, b_2]$ is a reduced basis, then b_1 is a shortest nonzero vector in L.

Proof. (Following Borevich and Shafarevich, Number Theory, p. 148) Without loss of generality we can take $b_1 = 1$. Let $b_2 = \alpha + \beta i$. Clearly b_1 is shortest among nonzero multiples of b_1, so we can consider $v = x + y(\alpha + \beta i)$ with $y \neq 0$. If $y = \pm 1$ then

$$|v|^2 = (x + \alpha)^2 + \beta^2 \geq \alpha^2 + \beta^2 \geq 1,$$

whereas otherwise

$$|v|^2 \geq y^2\beta^2 \geq 2\beta^2 \geq \alpha^2 + \beta^2 \geq 1.$$

Historical Notes

The notion of reduced basis seems to be due to R. Dedekind, following earlier work on quadratic forms by Lagrange, Gauss, and others. See Dickson, History of the Theory of Numbers, V. III.