CSE 206A: Lattice Algorithms and Applications Spring 2007

Lecture 3: Minimum distance

Lecturer: Daniele Micciancio *Scribe: Daniele Micciancio*

In this lecture we start studying a fundamental parameter associated to a lattice: its minimum distance. For any lattice $\Lambda = \mathcal{L}(\mathbf{B})$, we define the minimum distance of Λ and the smallest distance between any two lattice points:

$$\lambda(\Lambda) = \inf\{\|\mathbf{x} - \mathbf{y}\| \colon \mathbf{x}, \mathbf{y} \in \Lambda, \mathbf{x} \neq \mathbf{y}\}.$$

Computing the minimum distance of a lattice (and vectors achieving the minimum distance) is a fundamental problem in the algorithmic study of lattices, and the core of many applications in computer science and cryptography. Today, we will focus on mathematical properties of lattices, and answer questions like: is the quantity $\lambda(\Lambda)$ always achieved by a pair of vectors? (I.e., can the inf in the definition be replaced by min?) Does the minimum distance of a lattice satisfy interesting upper or lower bounds? We will also see how simple bounds on the minimum distance of a lattice be used to prove seemingly unrelated mathematical facts like the following.

Theorem 1 *Every prime number p congruent to 1 modulo 4, is the sum of two squares $p = a^2 + b^2$.*

We observe that the minimum distance can be equivalently defined as the length of the shortest nonzero lattice vector:

$$\lambda(\Lambda) = \inf\{\|\mathbf{v}\| \colon \mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}\}.$$

This follows from the fact that lattices are additive subgroups of $\mathbb{R}^n$, i.e., they are closed under addition and subtraction. So, if $\mathbf{x}$ and $\mathbf{y}$ are distinct lattice points, then $\mathbf{x} - \mathbf{y}$ is a nonzero lattice point.

1 Lower bound

The first thing we want to prove about the minimum distance is that it is always achieved by some lattice vector, i.e., there is a lattice vector $\mathbf{x} \in \Lambda$ of length exactly $\|\mathbf{x}\| = \lambda(\Lambda)$. To prove this, we need first to establish a lower bound on $\lambda(\Lambda)$.

Proposition 2 *For every lattice basis $\mathbf{B}$ and its corresponding Gram-Schmidt orthogonalization $\mathbf{B}^*$*

$$\lambda = \inf\{\|\mathbf{v}\| : \mathbf{v} \in \mathcal{L}(B)/\{\mathbf{0}\}\} \geq min\|\mathbf{b}_i^*\|.$$

Proof Note that $\mathbf{b}_i^*$ are not lattice vectors. Let us consider a generic lattice vector

$$\mathbf{Bx} \in \mathcal{L}(\mathbf{B})/\{\mathbf{0}\},$$

where $\mathbf{x} \in \mathbb{Z}^n/\{\mathbf{0}\}$ and let k be the biggest index such that $x_k \neq 0$. We prove that

$$\|\mathbf{Bx}\| \geq \|\mathbf{b}_k^*\| \geq \min_i \|\mathbf{b}_i^*\|. \tag{1}$$

In order to prove (1), we take the scalar product of our lattice vector and $\mathbf{b}_k^*$. Using the orthogonality of $\mathbf{b}_k^*$ and $\mathbf{b}_i$ (for $i < k$) we get

$$\begin{aligned} \langle B\mathbf{x}, \mathbf{b}_k^* \rangle &= \sum_{i \leq k} \langle \mathbf{b}_i x_i, \mathbf{b}_k^* \rangle \\ &= x_k \langle \mathbf{b}_k, \mathbf{b}_k^* \rangle = x_k \|\mathbf{b}_k^*\|^*. \end{aligned}$$

By Cauchy-Shwartz,

$$\|\mathbf{Bx}\| \cdot \|\mathbf{b}_k^*\| \geq |\langle \mathbf{Bx}, \mathbf{b}_k^* \rangle| \geq |x_k| \cdot \|\mathbf{b}_k^*\|^2.$$

Using $|x_k| \geq 1$ and dividing by $\|\mathbf{b}_k\|^*$, we get $\|\mathbf{Bx}\| \geq \|\mathbf{b}_k^*\|$. ■

Notice that the lower bound $\min_i \|\mathbf{b}_i^*\|$ depends on the choice of the basis. We will see later in the course that some bases give better lower bounds than others, but at this point any nonzero lower bound will suffice. We want to show that there is a lattice vector of length λ. Consider a sphere of radius 2λ. Clearly, in the definition of $\lambda = \inf\{\|\mathbf{x}\| : \mathbf{x} \in \Lambda \setminus \{0\}\}$, we can restrict $\mathbf{x}$ to range over all lattice vectors inside this sphere. We observe that (by a volume argument) the sphere contains only finitely many lattice points. (Details below.) It follows that we can replace the inf operation with a min, and there is a point in the set achieving the smallest possible norm.

How can we use a volume argument, when points have volume 0? Put an open sphere or radius $\lambda/2$ around each lattice point. Since lattice points are at distance at least λ, the spheres are disjoint. The spheres with centers in S are also contained in a sphere S' of radius 3λ. So, since the volume of the small spheres (which is proportional to $1/2^n$) cannot exceed the volume of the big sphere S' (which has volume proportional to 3^n), there are at most 6^n lattice points.

2 Upper bound

We now turn to estimating the value of λ from above. Clearly, for any basis $\mathbf{B}$, we have $\lambda(\mathbf{B}) \leq \min_i \|\mathbf{b}_i\|$, because each column of $\mathbf{B}$ is a nonzero lattice vector. We would like to get a better bound, and, specifically, a bound that does not depend on the choice of the basis. We will prove an upper bound of the form $\lambda(\Lambda) \leq \alpha(n) \det(\Lambda)^{1/n}$.

Why $\det(\Lambda)^{1/n}$? The reason we look for bounds of this form is that the expression $\det(\Lambda)^{1/n}$ scales linearly with the lattice, i.e., if we multiply a lattice by a factor c, then we obtain $\lambda(c\Lambda) = c\lambda(\Lambda)$ and $\det(c\Lambda)^{1/n} = c\det(\Lambda)^{1/n}$.

The upper bound on $\lambda(\Lambda)$ we are going to prove was originally proved by Minkowski. Here we follow a different approach, by first proving a theorem of Blichfeldt from which Minkowski's theorem can be easily derived as a corollary.

Theorem 3 (Blichfeldt theorem.) *Given a lattice $\mathcal{L}(B)$ and a set $S \subseteq \mathbb{R}^m$ if vol$(S) >$ $\det(B)$ then S contains two points $z_1, z_2 \in S$ such that $\mathbf{z}_1 - \mathbf{z}_2 \in \mathcal{L}(B)$.*

Proof Consider the sets $S_{\mathbf{x}} = S \cap (\mathbf{x} + \mathcal{P}(B))$, where $\mathbf{x} \in \mathcal{L}(B)$. Notice that these sets form a partition of S, i.e., they are pairwise disjoint and

$$S = \bigcup_{x \in \mathcal{L}(B)} S_x.$$

In particular we have

$$\mathrm{vol}(S) = \sum_{\mathbf{x} \in \mathcal{L}(B)} \mathrm{vol}(S_{\mathbf{x}}).$$

Notice that the transtated sets $S_{\mathbf{x}} - \mathbf{x} = (S - \mathbf{x}) \cap \mathcal{P}(B)$ are all contained in $\mathcal{P}(B)$. We want to prove that the $S_{\mathbf{x}}$ cannot be all mutually disjoint. Since $\mathrm{vol}(S_x) = \mathrm{vol}(S_{\mathbf{x}} - \mathbf{x})$, we have

$$\mathrm{vol}(\mathcal{P}(B)) < \mathrm{vol}(S) = \sum_{x \in \mathcal{L}(B)} \mathrm{vol}(S_x) = \sum_{x \in \mathcal{L}(B)} \mathrm{vol}(S_{\mathbf{x}} - \mathbf{x}).$$

The facts that $S_{\mathbf{x}} - \mathbf{x} \subseteq \mathcal{P}(B)$ and $\sum_{x \in \mathcal{L}(B)} \mathrm{vol}(S_{\mathbf{x}} - \mathbf{x}) > \mathrm{vol}(\mathcal{P}(B))$ imply that these sets cannot be disjoint, i.e. there exist two distinct vectors $\mathbf{x} \neq \mathbf{y} \in \mathcal{L}(B)$ such that $(S_{\mathbf{x}} - \mathbf{x}) \cap (S_{\mathbf{y}} - \mathbf{y}) \neq 0$.

Let $\mathbf{z}$ be any vector in the (non-empty) intersection $(S_{\mathbf{x}} - \mathbf{x}) \cap (S_{\mathbf{y}} - \mathbf{y})$ and define

$$\mathbf{z}_1 = \mathbf{z} + \mathbf{x} \in S_{\mathbf{x}} \subseteq S$$

$$\mathbf{z}_2 = \mathbf{z} + \mathbf{y} \in S_{\mathbf{y}} \subseteq S.$$

These two vectors satisfy

$$\mathbf{z}_1 - \mathbf{z}_2 = \mathbf{x} - \mathbf{y} \in \mathcal{L}(B).$$

■

As a corollary to Blichfeldt theorem we immediately get a theorem originally due to Minkowski that gives a bound on the length of the shortest vector in a lattice.

Corollary 4 (Minkowski's convex body theorem) *If S is a convex symmetric body of volume vol$(S) > 2^m \det(B)$, then S contains a non-zero lattice point.*

Proof Consider the set $S/2 = \{\mathbf{x} : 2\mathbf{x} \in S\}$. The volume of $S/2$ satisfies

$$\mathrm{vol}(S/2) = 2^{-m}\mathrm{vol}(S) > \det(B)$$

By Blichfeldt theorem there exist $z_1, z_2 \in S/2$ such that $\mathbf{z}_1 - \mathbf{z}_2 \in \mathcal{L}(B) \setminus \{\mathbf{0}\}$. By definition of S/2, $2\mathbf{z}_1, 2\mathbf{z}_2 \in S$. Since S is symmetric, also $-2\mathbf{z}_2 \in S$ and by convexity,

$$\mathbf{z}_1 - \mathbf{z}_2 = \frac{2\mathbf{z}_1 - 2\mathbf{z}_2}{2} \in S$$

is a non-zero lattice vector contained in the set S. ■

The relation between Minkowski theorem and bounding the length of the shortest vector in a lattice is easily explained. Consider first the ℓ_∞ norm: $\|\mathbf{x}\| = \max_i |x_i|$. We show that every (full rank, n-dimensional) lattice Λ always contains a nonzero vector $\|\mathbf{x}\| \leq$

$\det(\Lambda)^{1/n}$. Let $l = \min\{\|\mathbf{x}\|_\infty : \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}\}$ and assume for contradition $l > \det(\Lambda)^{1/n}$. Take the hypercube $C = \{\mathbf{x} : \|\mathbf{x}\| < l\}$. Notice that C is convex, symmetric, and has volume $\mathrm{vol}(C) = (2l)^n > 2^n \det(\Lambda)$. So, by Minkowski's theorem, C contains a nonzero lattice vector $\mathbf{x}$. By definition of C, we have $\|\mathbf{x}\|_\infty < l$, a contradiction to the minimality of l.

Corollary 5 *For any full dimensionsional $\mathcal{L}(B)$ there exists a lattice point $x \in \mathcal{L}(B)/\{0\}$ such that*

$$\|\mathbf{x}\|_\infty \leq \det(\mathbf{B})^{1/n}.$$

Using inequality $\|\mathbf{x}\| \leq \sqrt{n}\|\mathbf{x}\|_\infty$ (valid for any n-dimensional vector $\mathbf{x}$, we get a corresponding bound in the ℓ_2 norm.

Corollary 6 *For any full dimensionsional $\mathcal{L}(B)$ there exists a lattice point $x \in \mathcal{L}(B)/\{0\}$ such that*

$$\|\mathbf{x}\|_\infty \leq \sqrt{n}\det(\mathbf{B})^{1/n}.$$

It is easy to see that for Euclidean norm the full dimensionality condition is not necessary.

We could have proved the bound for the Euclidean norm directly, using a sphere instead of a cube, and then plugging in the formula for the volume of an n-dimensional sphere. This can be useful to get slighly better bounds. For example, in two dimensions, for any lattice Λ, the disk $S = \{\mathbf{x} : \|\mathbf{x}\| < \lambda(\Lambda)\}$ contains no nonzero lattice point. So, by Minkowki's theorem, the area of S can be at most $2^n \det(\Lambda) = 4\det(\Lambda)$. But we know that the area of S is $\pi\lambda^2$. So, $\lambda(\Lambda) \leq 2\sqrt{\det(\Lambda)/\pi}$, which is strictly smaller than $\sqrt{2}\det(\Lambda)^{1/n}$.

We remark that a lattice Λ can contain vectors arbitrarily shorter than Minkowski's bound $\sqrt{n}\det(\Lambda)^{1/n}$. Consider for example the two dimensional lattice generated by the vectors $(1,0)^T$ and $(0,N)^T$, where N is a large integer. The lattice contains a short vector of length $\lambda = 1$. However, the determinant of the lattice is N, and Minkowski's bound $\sqrt{2}N^{1/2}$ is much larger than 1.

It can also be shown that Minkowski's bound cannot be asymptotically improved, in the sense that there is a constant c such that for any dimension n there is a n-dimensional lattice Λ_n such that $\lambda(\Lambda) > c\sqrt{n}\det(\Lambda)^{1/n}$. (See homework assignment.) So, up to constant factors, $O(\sqrt{n})\det(\Lambda)^{1/n}$ is the best upper bound one can possibly prove on the length of the shortest vector of any n-dimensional lattice.

3 An application

We are now ready to prove that any prime number p congruent to 1 mod 4 can be written as the sum of two squares.

Theorem 7 *For every prime $p \equiv 1 \bmod 4$ there exist integers $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$*

Proof Let $p \in \mathbb{Z}$ be a prime such that $p \equiv 1 \bmod 4$. Then $\mathbb{Z}_p^*$ is a group such that $4 \mid o(\mathbb{Z}_p^*) = p - 1$. Therefore, there exists an element of multiplicative order 4, and -1 is a quadratic residue modulo p, i.e. there exists an integer i such that $i^2 \equiv -1 \pmod{p}$. It immediately follows that

$$p \mid i^2 + 1. \tag{2}$$

Now define the lattice basis

$$\mathbf{B} = \left[\begin{array}{cc} 1 & 0 \\ i & p \end{array} \right].$$

By Minkowski's theorem there exists an integer vector $\mathbf{x}$ such that $0 < \|B\mathbf{x}\|_2 < \sqrt{2} \cdot \sqrt{\det(B)}$. Squaring this equation yields

$$0 < \|B\mathbf{x}\|_2^2 < 2 \cdot \det(B) = 2p. \tag{3}$$

The middle term expands to

$$\left\| \left[\begin{array}{c} x_1 \\ ix_1 + px_2 \end{array} \right] \right\|^2 = x_1^2 + (ix_1 + px_2)^2 \tag{4}$$

If we let $a = x_1$ and $b = ix_1 + px_2$, (2) becomes

$$0 < a^2 + b^2 < 2p \tag{5}$$

Hence if we can show that $a^2 + b^2 \equiv 0 \mod p$, by necessity $a^2 + b^2 = p$.

Expanding the right side of (3) produces $x_1^2 + i^2x_1^2 + p^2x_2^2 + 2ix_1px_2$, which can be factored into

$$p(px_2^2 + 2ix_1x_2) + x_1^2(i^2 + 1)$$

Obviously p divides the first term, and by (1) p divides the second term. Thus $a^2 + b^2 \equiv 0 \mod p$, and therefore by (4) $a^2 + b^2 = p$. ■

You see how lattices can be used to prove non-trivial facts in number theory. A similar theorem that can be proved with the same lattice techniques is the following.

Theorem 8 $\forall n \in \mathbb{Z}^+ \; \exists a, b, c, d \in \mathcal{Z} : n = a^2 + b^2 + c^2 + d^2$.

As you can easily guess, the proof involves 4-dimensional lattices.